ICT-31-2014: Human-centric Digital Age
Project number: 645043

A typology, method and roadmap for HUman-MAchine NEtworks

Deliverable D4.1

Report on implications of future thinking

Editor(s)	Eva Jaho
Lead Partner	ATC
Version	11
Date	07/10/2016
EC Distribution	Public

Project Number	H2020 – 645043
Project Title	HUMANE

Title of Deliverable	Report on implications of future thinking
Date of delivery to the EC	07/10/2016

Editor(s)	Eva Jaho
Contributors	Eric T. Meyer (UOXF) Brian Pickering (IT Innovation) Paul Walland (IT Innovation) Till Christopher Lech (SINTEF) Asbjørn Følstad (SINTEF) Nikos Sarris (ATC)
Reviewer	Taha Yasseri (UOXF)

Abstract	An important goal in the HUMANE project is to set out the implications for future thinking and policy making in Human-Machine Networks (HMN). In this deliverable, we explore relevant characteristics and implications of HMNs in a number of innovative domains that have high potential for bringing fundamental social changes: the sharing economy, eHealth, citizen participation, telework, workplace robotics, and crowd management. We also identify potential challenges and obstacles, as well as possible ways to mitigate these in future ICT R&I projects. Our work is positioned relative to the general EU priorities and relevant strategy plans. We review future opportunities and recommendations for R&I actions.
Key-words	Human-machine networks, stakeholders, implications, challenges, future-thinking

Versioning and contribution history

Version	Date issued	Description	Contributors
V01	12.05.2016	Outline	ATC
V02	31.05.2016	Extended outline following partner input	ATC, all
V03	12.07.2016	Integrating new partner input, sections 4.2, and 4.4	ATC
V04	25.07.2016	Integrating new partner input, section 2	ATC
V05	04.08.2016	Integrating new partner input, section 6	UOXF
V06	12.08.2016	Integrating new partner input, sections 4.3 and 4.6	IT Innovation
V07	25.08.2016	Integrating new partner input, section 4.1	SINTEF
V08	09.09.2016	Integrating new partner input, sections 3 and 5	ATC
V09	15.09.2016	Integrating new partner input, sections 1 and 4.5	ATC
V10	23.09.2016	Draft submitted to internal review	ATC, all
V11	07.10.2016	Updated version following internal reviewer comments	ATC, all

Definitions and abbreviations

Abbreviation	Definition
CC	Collaborative Consumption
DSS	Decision Support System
ECG	Electrocardiography
EHRs	Electronic Health Records
HMN	Human Machine Network
HRI	Human Robot Interaction
H2M	Humane to Machine
ICT	Information and Communication Technology
QoS	Quality of Service
R&I	Research and Innovation
SWHS	Smart Wearable Health Systems
VPN	Virtual Private Network
WHO	World Health Organization

Executive summary

In the emerging hyper-connected era, work, private life, civic engagement, creativity and innovation are increasingly conducted in communication networks consisting of humans and machines. Machines interact with humans in increasingly important ways, in almost every aspect of human life and society: economy, health, work, governance, as well as human relationships. This has been the motivation for defining and analysing Human-Machine Networks (HMNs). In the course of the HUMANE project, we provide a framework and method for classifying and analysing the characteristics of such networks, and study how we can inform design and policy making so that we maximize societal benefits.

In previous work of the HUMANE project, we have performed a comprehensive literature review (HUMANE deliverable D1.1), defined a typology and method to support analysis and design of HMNs (HUMANE deliverable D2.2), and examined specific test cases (HUMANE deliverable D3.2). Building on this work, we in this deliverable go beyond studies of specific applications and examine the broader impact and implications of HMNs in social domains, the technical and regulatory challenges that we encounter, and report on policy interventions that can help to overcome these challenges and accomplish the desired design goals. The purpose of this, is to provide a baseline for the upcoming work in HUMANE on developing roadmaps for future HMNs.

We examine the following six domains: the sharing economy, eHealth, citizen participation, workplace robotics, telework, and decision support systems (DSS) for crowd management. These are domains embracing exciting technological applications, which promise to bring great benefits to the economy and society. From a HMN perspective they cover a broad range of modalities of relevance to the HUMANE typology, such as for HMN dimensions pertaining to human and machine agency, the relation or tie strength between the human and the machine actors in the network, as well as organization and extent of the networks. The targeted domains have also been identified as potential drivers for growth and are abundant fields for research and policy making.

For each of the above domains, we describe the policy background and current initiatives, identify stakeholders and describe their roles and interests. Moreover, we examine the technical and non-technical challenges, and demonstrate opportunities for policy intervention. We also provide a summary of key challenges and objectives across different fields and their implications for HMN design. Finally, we provide future policy interventions and recommendations for R&I actions.

We find that key technical challenges in different domains are data security, scalability, and efficient collaboration environments and tools. Data security may significantly affect privacy and trust, and may implicitly affect users' motivation for a high level of engagement in HMNs. Scalability usually involves the efficient handling of significant amounts of data, but it may also involve the communication infrastructure, as in the scaling of a VPN for a very large number of teleworkers, or the control of a large number of robots. Effective scaling of HMNs may also improve user experience and mitigate information overload. Efficient collaboration may involve different challenges depending on the purpose of the HMN. Networks that facilitate long term work engagements, e.g., within telework, may hold different requirements than networks that require more urgent response, such as DSS.

Lacks in legislation or fragmented regulations have been identified as potential issues in all domains. For example, lack of legal clarity exists regarding the marketing and validity of eHealth applications, and fragmented regulations were identified in the sharing economy, which may create confusion and endanger competitiveness. A recurrent issue is also the provision of sustainable business models, since HMNs require high cost for setting up the infrastructure, operation and maintenance; without sustaining the cost, HMNs risk to create a technological divide between classes of people. Finally, ethical issues were identified for robotic systems and decision support systems for crowd management.

We suggest a number of policy interventions that can promote beneficial HMNs in these domains. For example, in the sharing economy, a regulatory environment that promotes growth could benefit from emphasizing data protection and facilitate the sharing of assets. In eHealth, future HMN development could benefit from clearer rules for the management of medical data and the regulation of eHealth applications. In addition, it may be beneficial for regulation to support the development of more reliable network infrastructures for guaranteed quality of service, availability, and low latency required for critical tasks such as telesurgery. Citizen participation may benefit from policy interventions concerning opening data in a transparent manner, and supporting participation of under-represented groups. In telework, we have suggested that policy interventions could be useful to address large inequalities across employment fields and countries and gaps in regulation concerning compensation, work arrangements, taxation regimes, health and safety, and privacy and personal data protection of teleworkers. In robotics, there may be a need for explicit consideration of ethics in research, development and marketing. A broader discussion should include the types of labour that can and should be carried out by robots (and conversely, those that should not be). These discussions should also take into account societal concerns about unemployment, inequality and equal access to the benefits of automation. Finally, relevant interventions in DSS for crowd management may include establishing norms related to crowd monitoring and response, establishing mechanisms for cooperative responses and ensuring that responsibility for intervention lies at the side of human actors.

The results derived in this deliverable form the basis on which to develop HUMANE roadmaps for each domain of interest. The implications for future thinking and policy-making on future ICT will be formulated as an easily accessible roadmap for future HMNs in different social domains, focusing on the goals to reach in each domain and the steps to achieve these goals.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Introduction

Future thinking on technological innovations implies examining the way a new technology is integrated in a human social environment and its potential long-term impact; how it would change human interactions and relationships, and what the effect would be on the economy and human development. This is usually done in early stages of a technology, before it is implemented at a large scale.

For understanding the characteristics and implications of Human-Machine Networks (HMNs), it is thus necessary to study specific applications of HMNs in specific social environments or domains and see what the impact will be, but also what are the desired goals and how we can intervene or facilitate their achievement.

In this deliverable we perform an in-depth study of innovative applications in social domains where HMN applications have a great potential for social change. In doing so, we improve our understanding of the characteristics and implications of HMNs, we identify potential challenges in the design of an HMN and report on policy interventions that can help to overcome these challenges and accomplish the desired goals of the application.

The chosen domains are: the sharing economy, eHealth, citizen participation, workplace robotics, telework, and decision support systems for crowd management. These domains embrace exciting technological applications, which promise to bring great benefits to the economy and society. They are a set of diverse domains, differing in HMN characteristics, such as the levels of human and machine agency, the human-to-human and human-to-machine ties and interaction strength, or the network size and coverage. By choosing this diverse set of domains, we aim to explore the major transformations induced by digitalisation in human relations, governance, the economy, the organisation of work, as well as the production of knowledge and social capital.

The present study is the first step towards developing roadmaps for HMN applications. The roadmaps can act as a reference on which a collaborative effort, such as the one needed for finding and implementing efficient policies for HMNs, can be based. It helps all the involved parties recognize the goals and the steps needed for their achievement, and better understand their roles and interrelations. HUMANE roadmaps will be constructed for some of the above domains. Each roadmap will consist of the goals to reach in each selected social domain and the required actions to achieve each goal, potentially as a number of separate steps.

Our study is closely linked to EC's policies and strategies, in particular the new Digital Single Market strategy.[1] Each of the above domains has attracted the interest of the EC's policy makers as a potential driver for growth. Therefore, it will be primarily useful to policy makers, who can obtain an overview of the current status and challenges of HMN applications, see interrelations between similar HMN applications in different domains and integrate the identified policy interventions in their agenda.

[1] http://ec.europa.eu/priorities/digital-single-market_en

During roadmap construction, we aim to exchange extensively with policy makers in order to find the best way to implement policies to address the future needs.

Apart from serving as a basis for the roadmaps, the approach taken in this deliverable to study a social domain (describing the topic, the involved stakeholders and roles, specific challenges and objectives, policy background and opportunities for policy interventions) can serve as a model for the analysis of other domains, so that a rich repository can be created that will guide future policy making.

Furthermore, the findings in this deliverable will be interesting for professionals working in one of the examined domains, ICT experts, or researchers. It offers a holistic view of technological developments, technical and non-technical challenges, the regulatory background and needs, linking them to a typology and general characteristics of HMNs.

The structure of this deliverable is as follows:

In Section 2 we present, as background, a short description of HMNs in the context of HUMANE project, the priorities set in general by the EU and the current strategic plans. We discuss the expected growing importance of HMNs in different domains and the possible role of HMNs in achieving the objectives, as well as the need for future thinking and roadmaps. We explain the reasons for focusing on these domains, which lie in their central role in the Digital Single Market strategy and the expected growing importance of HMNs in such domains. In Section 3, we describe the general categorization of relevant stakeholders: policy makers, professionals, IT experts, and research experts. This categorization is the same for every domain, although representatives in each category will differ for each domain. However, the stakeholders in each category share common attributes, as to why HMNs are important to them and why the future thinking and roadmaps would help them. Section 4 is the main section of the deliverable, where for each domain we describe the HMNs that are encountered, present the stakeholders, their role and interests, describe technical and non-technical challenges, the policy background and current initiatives, and identify opportunities for policy intervention.

In Section 5 we provide a general view of the technical (e.g. security and privacy, scalability, availability) and non-technical (e.g. development of business models, support of standardization activities, actions for public awareness) challenges. We also provide the requirements to successfully confront them, including a summary of common challenges and objectives in different domains, according to different typologies of HMNs. Following this, we identify in Section 6 the required interventions in general, as well as recommendations for R&I actions. Finally, in the conclusion (Section 7), we summarize the work in this report and point forward to the roadmap that will be developed within HUMANE.

2 Background

2.1 Human-Machine Networks

HMNs are networks composed of humans and machines that interact to produce synergistic effects. They have been conceptualized due to the increasingly important role of machines with processing and communication capabilities in modern society; when viewed as agents or nodes in a network, such machines mediate or effect many human actions and exercise significant influence. For example, modern initiatives to address environmental problems are executed in networks involving government, private firms and citizens, but also smart devices and sensor networks. Systems for emergency response and rescue involve complex interactions between sensors, smart machines, and emergency response teams. Education and work is increasingly conducted from a distance using collaborative software.[2]

An individual that lives in such an environment does not only need to learn how to interact with other people, but also how to use or interact with the machines in his environment. The outcome of a human action may in part be determined by the capabilities or constraints of a machine. The study of HMNs is important in order to better design machines so that they fulfill human and societal needs (human-centered design), but also in order to help human societies adjust to the new human-machine environment and maximize positive synergistic effects.

Within the HUMANE project we have developed a framework for studying HMNs that consists of a typology of HMNs and a method for creating HMN profiles that can support the analysis, requirements collection, design, and evaluation of such networks. The typology consists of different dimensions, such as human and machine agency, tie and interaction strength, network size and geographical expansion, workflow interdependence and network organization.[3] These are organized into abstract layers of actors, interactions, and layers of network and behavior characteristics. The abstraction helps to identify similarities and differences between HMNs, and understand implications of HMNs (i.e. effects on motivation, trust, shared responsibility, privacy, etc.) that can help to guide the design process.

The typology also serves as guidance for examining social domains we study in this deliverable. In each social domain, we try to characterize HMN dimensions and describe implications of current design.

2.2 Policy background and current initiatives

The policy background for regulating digital communications and services in Europe has included a wide range of laws and directives. For example, relevant for HMNs are the Data Protection Directive (95/46/EC) and the General Data Protection Regulation (Regulation (EU) 2016/679), the Machinery Directives (8/37/EC and 2006/42/EC), and the Directive on security of network and information systems (DIRECTIVE (EU) 2016/1148). The increasingly predominant role of the Internet and digital technologies, which makes it possible to provide advanced data communications and facilitate the exchange of goods and services, has motivated the European Commission to develop a strategy that can provide common rules for the digital market across Europe and exploit the advances of technology to the benefit of European citizens. This strategy, called the European Digital Single Market, is made up of three policy areas or “pillars”:

[2] Understanding Human-Machine Networks: A Cross-Disciplinary Survey. Tsvetkova, Milena, et al. (2015) Available on line: https://arxiv.org/abs/1511.05324
[3] Deliverable D2.2: “Typology and method”. Humane Project (2016)

- **Better online access to digital goods and services**: It covers topics in e-commerce, helping to make the EU's digital world a seamless and level marketplace to buy and sell. This has ramifications that extend well beyond financial transactions, aiming to remove the key differences between online and offline worlds, and break down barriers to cross-border online activity.
- **An environment where digital networks and services can prosper**: Designing rules which match the pace of technology and support infrastructure development. In this respect, the Digital Single Market aims to provide high-speed, secure and trustworthy infrastructures and services supported by the right regulatory conditions. It provides rules for protection of open Internet access, a review of the audiovisual media framework, rules for online platforms (search engines, social media, app stores, etc.), e-privacy and cybersecurity.
- **Digital as a driver for growth**: Ensuring that Europe's economy, industry and employment take full advantage of what digitalisation offers. It proposes an initiative for the free flow of data within the EU and the creation of **standards that facilitate interoperability** in areas critical to the Digital Single Market, such as e-health, transport planning or energy (smart metering), and e-government actions. Digitalisation also induces major transformations in the organisation of work and employment relationships. This includes new ways of working flexibly and new types of employment relationships, such as telecommuting or telework, freelance work or independent professionals, crowdsourcing and employment in the sharing economy.

The Digital Single Market strategy aims to enable the EU to become a (1) smart, (2) sustainable and (3) inclusive economy. These three mutually reinforcing priorities should help the EU and the Member States deliver high levels of employment, productivity and social cohesion.[4] Europe's average growth rate has been structurally lower than that of its main economic partners (primary USA and Japan), mainly due to differences in business structures combined with lower levels of investment in R&D and innovation, insufficient use of information and communication technologies, reluctance to embrace innovation, barriers to market access and a less dynamic business environment.

We advocate that understanding the implications that current policies have on the design of HMNs is a central part of this effort. Improving EU competence in digital technologies does not only call for an increase in investment in research and development. The implementation of the Digital Single Market strategy goes beyond the mere application of technological advances in real life and economy, but requires the study of how future technology will be integrated in social environments. It is necessary to understand the implications brought by new technologies in critical social domains, and anticipate the future evolution. The future world will consist of various HMNs that interlink humans and machines in complex ways, which we need to understand and adapt to. Future machines, equipped with computational logic and various communication interfaces, become more automated, decrease direct human-to-human communication and interact not only with humans but also with each other in carrying out tasks that would otherwise require significant time and effort.

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF

2.3 The need for future policies, future-thinking and roadmaps of HMNs

Apart from making HMNs functional and designing human-machine interfaces presenting ergonomic properties such as friendliness and usability, the challenge is to examine how humans and machines interact in different social domains, what problems exist and how they can at best cooperate. The need for cooperation arises from the fact that humans are no longer in full control of the machines; we have long passed the era where computers were used for specific tasks, such as typesetting, calculation, programming, or design. Modern computational machines have a high degree of automation and are able to process data and take decisions on their own, without waiting for instructions in every step (Hoc, 2000). This creates the need for humans to rely on machines and to interact with them as if they were autonomous agents.

From the network viewpoint, the interactions of humans in a society are mediated, or highly influenced by machines. This affects societal domains such as health, economy, work, governance, and transforms norms of behavior. In order to ensure progress in such domains, many of the rules governing each domain have to be adapted, so that machines are integrated harmoniously in human life, but also humans adapt to certain machine behaviors and outputs. For example, in health, there has been significant technical progress in physiological monitoring with SWHS (Smart Wearable Health Systems and Applications), which help patients (or even healthy individuals) to monitor their health, transmit data from the sensing of physiological data to health professionals and help to improve life quality and reduce medical costs. However, the processing of medical information without adhering to strict privacy and security rules can significantly impede the functioning of such networks and discourage humans from using such devices. In another example, web 2.0 and high data speed technologies have given new dynamics to working from a distance (telework), enabling the reduction of work costs, reducing energy, and improving work-life balance. However, these new forms of labour remain marginalized and at the discretion of employers, and lacks the regulation and guidelines essential to legitimise it and enable its wider adoption. Moreover, robotic systems are gradually being introduced in human social environments and have a great potential to facilitate human labour and augment production. However, these systems are designed and sold with little or no ethical oversight, which may endanger the values and norms of human society.

Humans are also highly influenced by emotions or behavior characteristics such as trust, sense of responsibility, motivation, and concepts such as privacy, security, innovation. For example, the degree of trust or social responsibility may profoundly affect a HMN for collaborative work. Therefore, as mentioned in D2.2, we need new knowledge concerning how variations in HMNs affect these aspects. The HUMANE framework was developed to facilitate this analysis, and to easily find differences and commonalities between HMNs.

Unlike previous deliverables D3.1 and D3.2 where we performed specific case studies, here we examine important social domains, where human-machine interaction is expected to be significant in the future, and study in more detail the type of interactions, the roles of humans and machines, and the challenges that must be addressed to ensure the successful integration of machines that can be beneficial to the society. Our systematic approach will help to address these challenges by identifying opportunities for policy interventions, and setting objectives and specific milestones in the form of a roadmap for a specific domain.

2.4 Overview of the selected social domains

As explained in the Introduction (Section 1), we have chosen to perform an in-depth study of the following domains (cf. Section 4):

- sharing economy
- eHealth systems
- citizen participation
- telework
- human-robot networks
- decision support systems for crowd management

These social domains present innovative applications in the digital society with significant implications for future thinking. They share commonalities, but also HMN characteristics, so together they can cover a broad range of issues pertaining to HMNs and policy making.

First, we study in Section 4.1 how HMNs can enhance the access to goods and services in the sharing economy. The sharing economy (also called "collaborative economy") consists of the ecosystem of online collaboration, sharing, and collaborative consumption (CC). CC sites are alternative forms of online marketplaces where users can engage in peer-to-peer activities of obtaining, giving, or sharing the access to goods and services, coordinated through community-based online services. Similar to online marketplaces, people can provide information on their shared goods or provided services and the system can allow comparisons of prices and services, provide recommendations and reputation information. More generally, the various instances of the sharing economy also share the characteristics of online collaboration, online sharing, social commerce, and some form of underlying ideology, such as collective purpose or a common good (Hamari, Sj??klint, & Ukkonen, 2016). These platforms are in many ways a natural outgrowth of social media which bring together people with common interests to share not only ideas and information but also goods and services. The importance of the sharing economy lies in its ability to alleviate societal problems such as hyper-consumption, pollution, and poverty by lowering the cost of economic coordination within communities. The collaborative economy is small but growing rapidly, gaining important market shares in some sectors. Some experts estimate that the collaborative economy could add EUR 160-572 billion to the EU economy.[5] The recently published European Agenda for the collaborative economy[6] highlights this importance and presents key issues and challenges for a balanced provision of such services.

Next, we also study eHealth systems, a domain of great social importance where consistent rules must be set-up in the EU. eHealth services can benefit society by improving access to care, improving the

[5] A European agenda for the collaborative economy. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 2-6-2016

[6] http://ec.europa.eu/growth/single-market/strategy/collaborative-economy_en

quality of care and by making the health sector more efficient. eHealth includes information and data sharing between patients and health service providers, hospitals, health professionals and health information networks, electronic health records, telemedicine services, portable patient-monitoring devices, operating room scheduling software, robotized surgery and blue-sky research on the virtual physiological human. We identify challenges and barriers against the efficient management of eHealth systems, as well as opportunities and future policies that could support HMNs in this domain (see Section 4.2).

Another domain of interest we focus on, is citizen participation (see Section 4.3). Citizen participation systems are an extension of e-government systems whereby citizens perform the role of partner rather than customer in the delivery of public services, and change the traditional way that the public and the government interact. This can have tremendous benefits for improving democratic operation, building social cohesion and collective social capital. Yet individuals and citizen groups have a small part in decision making. Apart from voting for elections or referendums, citizen involvement in decision making is usually restricted to commenting in public consultations. Section 4.3 investigates the role of HMNs in building efficient citizen participation systems, leveraging on social media, collaborative tools and decision support systems.

We also investigate HMNs in telework, which includes methods, platforms and systems for working and cooperating with other workers from a distant location, via the use of ICT technologies. Although the concept of telework has been existing for more than 20 years, it has gained new dynamics from the proliferation of web technologies and high speed networks. Its benefits include decreasing traffic congestion and pollution by decreasing the number of commuters, reducing labour and overhead costs, such as costs for office space and operating/maintenance, offering more employment opportunities, and improving work and life balance. In Section 4.4 we investigate how we can confront the changing work structures that Internet technology brings through the proliferation of teleworking jobs, what kind of regulations lack, and what are the opportunities and benefits for the societies.

The domain of workplace robotics has to do with robots performing tasks requiring physical or mental effort, or facilitating humans in performing tasks. As mentioned in the Digital Single Market strategy[7] "t*he importance of robotics lies in its wide-ranging impact on Europe's capacity to maintain and expand a competitive manufacturing sector with millions of related jobs at stake. Robotics also offers new solutions to societal challenges from ageing to health, smart transport, security, energy and environment*". Benefits by robots include both the increase in productivity and improvement of quality of life, since robots can not only be used to automate production, but as house assistants, care givers, drivers, etc. In Section 4.5 we discuss technical and ethical challenges to better integrate robots in human social environments, and opportunities for policy interventions.

Decisions support systems (DSS) for crowd management emerge out of the need to handle emergency situations, but have evolved to cover a diversity of situations that require competencies in observing, sense-making, anticipating and acting. Examples include mass gatherings and demonstrations or evacuations in emergency scenarios. Despite criticisms for privacy violations and susceptibility to

[7] https://ec.europa.eu/digital-single-market/en/robotics

manipulation, DSS for crowd management can offer benefits such as improvement of public safety and prevention of dangerous situations, and can also be life-saving in disaster cases. In Section 4.6 we examine such systems within the framework of HMNs and present challenges and opportunities for policy interventions.

3 Relevant stakeholders

The inclusion of stakeholders is important in the work of the HUMANE project as they will have a central role in the development of roadmaps for HMNs in different social domains. During roadmap development, stakeholders will be consulted to discuss the current state of challenges, to further analyze and validate the roadmap goals, and produce a list of actions for the roadmap implementation.

For the HUMANE survey in Task 4.2 (D4.3), it will also be necessary to draw feedback on what stakeholders see as the most relevant, interesting, or promising HMNs in their field, (b) how do they characterize these HMNs and how do they expect these HMNs to evolve, (c) what do the stakeholders see as the key implications of how these HMN currently are operating or designed, and how they are evolving (e.g. in terms of user motivation, collaboration, innovation, privacy and trust, but also in terms of finance, employment etc.), and (d) which needs do the stakeholders see for technology innovation, or changes in policies and regulations. The identfication of the role and interests of stakeholders is necessary to prepare for this task.

Different stakeholders will appear in the different domains presented in Section 2.3. In general however, they can be categorized in the following classes:

- **Policy makers**: these are executives, managers, directors, and consultants, usually working in the public sector, who are interested in policy implications of HMNs and strategies to achieve the relevant objectives. Since identifying challenges and opportunities for policy interventions are the main purposes of the roadmaps, we consider this to be the primary group of interest.
- **Domain professionals**: professionals in relevant domains of interest for HMNs, who do not belong to any of the other groups: they are interested in applying best practices regarding HMNs in their daily practice. They have hands-on experience in the subject and can pinpoint practical problems that may be encountered in the implementation of a policy, as well as advantages and disadvantages of different policies.
- **User groups**: they are interested in adopting new technologies and familiarizing themselves with HMNs. The degree of adoption by the users is the key measure of success of any technology. Additionally, the familiarization of users with a certain technology is crucial in deciding the initial level of technology awareness, and the starting point of the roadmap, as well as the actions in order to reach the objectives. Apart from that, users can set requirements for a certain service or application, and pinpoint practical problems in policy implementation.
- **IT experts**: they are interested in design, capabilities and limitations of HMNs, and particularly the technical challenges, which much be faced in order to make HMNs perform more efficiently and respond to societal needs.

- **Researchers**: they are not only researchers in computer science and engineering, but also from fields such as sociology, psychology and political science, who are interested in challenges and future research on HMNs. Apart from the technical challenges, other challenges may include the ethical aspects of HMNs, the changes in human behavior, or structural changes in society as a result of HMNs.

The stakeholders in each domain are shown in Table 1.

Table 1: Stakeholders in each HUMANE domain of interest

	Policy makers	Domain experts	Users groups	IT experts	Research experts
Sharing economy	National governments, EU bodies	Companies, businesses	Consumers	IT experts in sharing economy	Researchers involved in new mechanisms and motivational factors fuelling the sharing economy
eHealth	National governments, EU bodies	Health professionals (both in-hospital (doctors, nurses, administrative) and out of hospital professionals (e.g. family doctor))	Patients and users groups: individuals, as well as groups representing patients	IT experts in eHealth: Companies developing eHealth applications, telemedicine systems, monitoring wearable devices	Computer scientists and engineers, researchers involved in patient management, care management and management of patient information
Citizen participation	Local and National Government, NGOs	Industries, security services	Political/ local/ interest groups	IT experts in data mining, content management , open data and security services	Researchers involved in citizen participation
Telework	National governments, EU bodies	Professionals in a certain labour domain (employees, employers)	Human resource experts	IT experts in collaboration and web conferencing tools, VPN technologies, secure email and instant	Computer scientists and engineers, civil and environmental engineers, sociologists, economists

	Policy makers	Domain experts	Users groups	IT experts	Research experts
				messaging applications, synchronization applications	
Workplace robotics	National governments, EU bodies	Professionals who interact with robots (e.g., doctors using robot to assist surgery, insurance companies who are likely to insure for damage caused by robots, logistics companies who may use robots for freight transport, or marketers working in robotic products)	Non-professional users, who interact with robots in normal activities (e.g., patients who use therapeutic robots, elderly people or people with disabilities who use care-robots, consumers who may encounter a robot-helper at a shopping mall)	Robotics manufacturers, IT experts involved in how a robot collects, processes and disseminates sensor data	Electoral and mechanical engineers, computer scientists, researchers in social sciences and humanities
Decision support for crowd management	National governments, NGOs	Operational staff, ancillary services (e.g., ambulance, police, fire service, terrorist units)	The Public in general	IT experts maintaining the infrastructure	Researchers in sensor networks, privacy, scalability etc.

Throughout the project, we plan to engage all stakeholders and provide channels of communication between the different groups of stakeholders. The stakeholder engagement will be pursued primarily through the organisation of joint workshops, where the roadmaps will be presented to policy makers in various iterations, and their feedback will be sought in order to align the roadmaps with their requirements and plans, and make them part of future policies.

4 Domains

In this section we perform an in-depth analysis of the selected domains, where for each domain we:

- describe HMN we encounter, the role of human and machine actors, as well as other HUMANE framework characteristics;
- present the different categories of stakeholders and discuss their role and significance, the approach towards them and the first plans for their involvement;

- describe the technical and non-technical challenges and the requirements to successfully confront them;
- describe the policy and regulatory background, the priorities set by the EU, current and previous R&I actions on these domains, and the current strategic plans, including the Digital Single Market strategy;
- identify opportunities for policy intervention, drawn from HMN implications and challenges, as well as shortcomings of current regulations. We discuss how the current regulations handle different aspects, such as trust, responsibility, security and privacy, user interaction, and also provide recommendations for R&I actions.

4.1 Sharing economy

4.1.1 Domain description

In recent years, especially following the aftermath of the financial crisis in 2008, there has been a growing trend towards individuals sharing physical and intellectual resources, enabled by HMNs such as online portals and collaboration platforms. Often summarised as "Sharing Economy" or "Collaborative Economy". The concept comprises four distinct elements (Botsman, 2013):

- Collaborative Economy: An economy built on distributed networks of connected individuals and communities versus centralised institutions, transforming how we can produce, consume, finance and learn.
- Collaborative Consumption: An economic model based on sharing, swapping, trading or renting products enabling access to ownership. It is reinventing not just what we consume but also how we consume.
- Sharing Economy: An economic model based on sharing underutilized assets, from physical space to human skills, or any items of monetary or non-monetary benefit.
- Peer Economy: Person-to-person marketplaces that facilitate the sharing and direct trade of products and services built on peer trust.

Common to these elements are the concepts of shared creation, production, distribution, trade and consumption of goods and services. For the sake of convenience, we will refer to the overall concept as sharing economy. Notable examples of the types of goods and services traded in the sharing economy are transportation (e.g. Uber and Zipcar), accommodation (e.g. AirBnB and Courchsurfing), as well as tools and other commodities (e.g. neighborgoods and streetbank). In general, high cost assets (cars and real estate) are most likely to yield economic value for temporal or permanent access or transfer of ownership, but recently, communities for sharing commodities are growing. Besides the economic benefit of sharing and re-using assets, users are increasingly drawn to collaborative consumption by a shifting attitude, moving towards anti-consumerism, green consumption and sustainability (Botsman & Rogers, 2010). A study by (Hamari et al., 2016) examining intrinsic and extrinsic motivational factors for engaging in the sharing economy suggests that sustainability and the enjoyment of being part of a community are important drivers. Regardless, the rapidly accelerating growth of the sharing economy has exceeded most expectations. A recent study by PwC [8] shows that the key sectors within the collaborative economy generated nearly €4bn in revenues and facilitated €28bn of transactions within Europe in 2015.

Human Machine Networks in the sharing economy: Technological development, most notably HMNs such as online communities, has undoubtedly been one of the most important drivers for the rise of the sharing economy. Nearly all platforms in the sharing economy are built upon apps or online tools for advertising and accessing the assets to be traded. Most of them are built upon successful platforms for online collaboration (Kaplan & Haenlein, 2010), fuelled by the widespread use of online communities and online social media. These tools and platforms vary extensively in their degree of sophistication, from applications with advanced built-in intelligence, such as recommendation engines and location-based services, to simple forum platforms such as Facebook groups.

HMNs in the sharing economy and the HUMANE typology: Despite a lot of commonalities between the various Human Machine Networks in the sharing economy, there are quite extensive differences both in behaviour, design and transaction workflows, depending on the kinds of products or services being traded. Naturally, a network offering the sharing of accommodation on a global base, will differ from a service for borrowing gardening tools within a neighbourhood. Therefore, an all-encompassing profile of the sharing economy as one phenomenon would fail to do justice to the complexity of the different networks.

However, within the different domains (exemplified by transport, accommodation, media /entertainment and commodities) certain consistencies can be identified as shown in the table below:

Analytical layer	Dimension	Transportation	Accommodation	Entertainment /media	Commodities
Actors	1. Human agency	Mid	Mid	Mid	Mid
	2. Machine agency	High	Mid	High	Mid
Interactions	3. Tie strength	Low	Low	Low	Mid
	4. H2M interaction strength	High	High	High	Mid
Network	5. Network size	High	High	High	High
	6. Geographical space	High-Low	High-Low	High	High-Low
Behaviours	7. Workflow inter-dependence	High	High	Mid	High
	8. Network organization	High-Low	High	High	Low

[8] Assessing the size and presence of the collaborative economy in Europe. PwC UK report. Available online: http://ec.europa.eu/DocsRoom/documents/16952/attachments/1/translations/en/renditions/native

This ad hoc profiling of different domains within the sharing economy shows some trends worth investigating in the further work towards a road map:

Trust: A striking trait of the sharing economy is that users engage with other users they do not know (i.e. low tie strength in the sharing economy HMNs) in trading and borrowing their assets (even high-cost assets like cars or housing). Both Botsman and Hamari's studies suggest that being a part of the same community, sharing other users' values and goals is one of the factors behind this level of trust. However, in line with the HUMANE typology, first interviews with businesses in the sharing economy point also to the high level of H2M interaction strength as another important dimension for trust in HMNs. The transaction processes of successful services in the sharing economy such as AirBnB or BlaBlaCar very often resemble the ones of known, commercial services (such as hotel booking sites or car rentals). Both have in common that these processes are rather deterministic, most often leading to a "buy"-button to be clicked in order to conclude a transaction. Services with less deterministic transaction processes (i.e. with less H2M interaction strength) such as Snapsale, which leaves the conclusion of a transaction to the users' discretion, report a higher threshold for users to conclude the transaction.

The interplay between H2M interaction strength, tie strength and human agency will be further investigated during the stakeholder interviews.

The role of Machine Agency: In the sharing economy, machine actors mostly have a role as mediator between supply and demand, matching the users' needs and interests with suitable offerings. However, the degree of intervention of networks in the exchange of goods, services and other assets varies widely from the pure matching services to all-encompassing platforms for matching, payment and user feedback. In terms of HMNs, machine agencies comprise mostly mobile apps or web sites serving as platforms that act as intermediaries between supply and demand.

4.1.2 Stakeholders involved in sharing economy

In the sharing economy, the following stakeholders can be identified:

- **Companies** running HMNs in the sharing economy.
- **Business associations** at national and European level, which need to ensure that there is a fair competition between the traditional consumer market and the sharing economy.
- **Consumers**, who need to be informed on the opportunities of participating in the collaborative economy, both in terms of economic benefits but also on the benefits of sustainable consumption.
- **IT experts**, who need to understand the sharing economy in order to put into place the necessary mechanisms for data protection and user-friendliness of platforms.
- **Research experts**, who need to produce more knowledge on the mechanisms and motivational factors fuelling the sharing economy.
- **Policy makers and regulatory bodies** at national and European level, who need to create the right framework conditions for a continuous growth.

The approach of working towards a road map for HMNs in the sharing economy will be based on three different phases. In the first phase, interviews will be conducted with companies and their IT experts, in order to learn more on their view on challenges, related to the market, technologies and regulations. The input from these interviews will in turn be a starting point for a dialogue with consumers and their views and expectations, policy makers and business associations in order to discuss regulative and policy implications (phase two). Finally, the results of the stakeholder dialogue will provide input to the final road map by determining required actions and design patterns in order to achieve the common goals of the stakeholders.

4.1.3 Specific challenges and high-level objectives of HMNs used in sharing economy

Start-up companies that pair innovative ideas with a suitable technical solution offer most of the services in the Shearing Economy. Very often however, services based on promising ideas will not prevail due to the lack of consideration of technical, as well as regulative issues. In the following, we present a preliminary list of challenges for the sharing economy.

Technical challenges:

- ***Data protection***: Solutions in the sharing economy must guarantee the security and integrity of their users' personal data.
- ***Scalability***: With the inherent network effects of the digital economy, solutions must be designed to manage a sudden large-scale increase of traffic and data once a service becomes viral.
- ***Availability***: Downtime of services may lead to loss of traffic and users. Solutions must be designed and maintained in a way that they guarantee maximum availability.
- ***Service design***: In order to attract and keep a critical mass of users, solutions with great attention to user interaction design, workflow design and usability must be implemented.

Non-technical challenges:

Despite the potential gains of the sharing economy in terms of economic growth and sustainability, there are some non-technical challenges that need to be overcome in order to enable further growth and a positive development:

- ***Regulation***: The current fragmented landscape in terms of rules, laws and regulation for the sharing economy may endanger Europe's competitiveness. The lack of unified regulations across Europe (the Digital Single Market) makes it difficult for services to expand across borders and gather critical mass. Currently, the European Union is determined to monitor these challenges, and if necessary, take legislative action in order to mitigate potential hinders for a sustainable development of the sharing economy (see Section 4.1.4).
- ***Business models***: In order to make any service in the sharing economy sustainable over time, business models need to be developed early in the process.
- ***Trust***: Both regulators and companies need more knowledge about the intrinsic mechanisms in the sharing economy that lead to trustful relations between users in order to implement regulations

fostering trust while protecting users and build services that utilize these mechanisms in order to build a strong customer base.

In Table 1 below we present a mapping of challenges to the relevant stakeholders.

Table 2 Challenges for sharing economy as they relate to specific stakeholders

	Companies	Business associations	Consumers	IT experts	Research experts	Policy makers
Data protection	X			X	X	X
Scalability	X			X		
Availability	X			X		
Service design	X			X	X	
Regulations	X	X	X		X	X
Business models	X	X	X			X
Trust	X		X		X	X

4.1.4 Policy background, current initiatives and future policies in sharing economy

The sharing economy is met by a patchwork of regulations in the different European Countries, ranging from market access requirements to data protection, protection of consumer rights and taxation. While some countries or cities (e.g. Berlin)[9] put restrictions in terms of frequency and duration of transactions on the sharing of accommodation in order to protect the access to affordable space for living, others (e.g. the City of London) encourage it.

On June, 2nd 2011, the European Commission released a communication "A European agenda for the collaborative economy"[10]. The communication describes the opportunity for both entrepreneurs and consumers. Nevertheless, it points out the importance of not letting the sharing economy become a parallel economy with its own rules. Certain key issues demand monitoring at the European level:

- Market access requirements – to what extent underlie sharing economy services market access requirements, such as authorisations, licensing obligations, etc.?
- Protection of users – in an environment that blurs the lines between traders and consumers, how to ensure the rights of the latter?
- Self-employed workers in the collaborative economy – how to ensure social protection of workers in the sharing economy?
- Taxation – how to avoid that the sharing economy becomes a parallel economy where taxation and other basic principles do not apply?

[9] "Zweckentfremdungsgesetz" in Berlin, Germany (https://service.berlin.de/dienstleistung/326217/)
[10] http://ec.europa.eu/DocsRoom/documents/16881

From the HMN viewpoint, the market access requirement is a highly relevant issue. The very design of a service in the sharing economy can, to a large extent, determine whether or not a service underlies market access requirements: The European Commission states that the degree of agency in a sharing economy HMN is a decisive factor in determining whether or not a HMN needs business authorisations and licenses in order to operate. In other words, networks that only match consumers and resources are regarded as information society service, whereas networks handling pricing, payment or even the delivery of services may need authorisation and licensing in accordance with relevant sector-specific regulation.

When it comes to the protection of users, the agenda for the collaborative economy encourages inherent mechanisms in HMNs for the protection of users, their data and commercial interests. Trust mechanisms, such as quality labels, should be improved to encourage users to engage in the sharing economy.

4.1.5 Opportunities for policy interventions in sharing economy

Based on this introduction to the topic, certain opportunities for policy intervention can be identified and will be used as input to the dialogue with stakeholders.

The first opportunity is related to Europe's strategic goals concerning sustainable growth. If the assumption holds true that both users and providers of services in the sharing economy share common goals and values when it comes to more responsible and sustainable consumption, there is a large potential in creating a regulatory environment that nourishes the growth of networks facilitating a collaborative use of assets.

Furthermore, in order to be competitive, Europe needs to accelerate the introduction of a Digital Single Market. While US services can gain their critical mass in a large homogeneous domestic market before taking on Europe, European providers struggle to extend their business across borders within the EU.

In addition, current European policy actions, such as the aforementioned Agenda for the Collaborative Economy, the Digital Single Market strategy, the new Data Protection regulation, as well as the strategy towards Digitising the European Industry will provide the policy framework for the stakeholder dialogue and further work on a road map for HMNs in the sharing economy.

4.2 eHealth

4.2.1 Topic description

According to the EU description[11], eHealth refers to tools and services using information and communication technologies (ICTs) that can improve prevention, diagnosis, treatment, monitoring and management of health issues. It includes information and data sharing between patients and health service providers, hospitals, health professionals and health information networks, electronic health records (EHR), telemedicine services, portable patient-monitoring devices, operating room scheduling

[11] http://ec.europa.eu/health/ehealth/policy/index_en.htm

software, robotized surgery and blue-sky research on the virtual physiological human. The European Commission in its eHealth Action Plan 2012-2020 defined eHealth as “using digital tools and services for health”, which is a generic term which covers different areas such as electronic health records, telemedicine, e-Prescription and m-Health.[12]

In a survey of research and development efforts in the EU, it was noted that, assisted by technological developments, the healthcare community is moving more toward early detection of diseases, health status monitoring, healthy lifestyle, and overall quality of life (Lymberis & Dittmar, 2007). eHealth services can benefit the entire community by improving access to care, quality of care and by making the health sector more efficient.

HMNs in eHealth include different systems and applications. Here we focus on electronic health records, telemedicine applications, and personalized monitoring devices (either stand-alone or networked devices).

An electronic health record describes the concept of a comprehensive, cross-institutional, collection of a patient’s health and healthcare data, in machine and human-readable forms. It includes historical data about a subject’s health condition and medical treatment. A more comprehensive definition also includes lifestyle and behavioral information captured personally by the individual or by a clinician, parent, or other caregiver (Waegemann CP., 1996). The eHealth record is meant to be used by the individual whom it concerns, health professionals involved in the treatment of the individual, as well as third parties involved in administrative support (health funds).

Telemedicine includes applications for training, advising, teleconferencing, and carrying out medical procedures such as surgical operations, and mainly involves the sending of real-time multimedia information about the patient and instructions for carrying out the procedure. On the other hand, robotized surgery concerns operations that may be carried out wholly or in part by machines.

Another application of HMNs concerns the physiological monitoring with SWHS (Smart Wearable Health Systems and Applications). Stand-alone devices for the measurement of vital signs like ECG (Electrocardiography), heart rate, respiratory rate, skin temperature, and posture (e.g. monitoring the body positions and movements for determining relationships to sleep apnea) are broadly used. Furthermore, current research is moving towards monitoring of multiple vital signals, as well as towards their use in a networked online environment, where sensor results can be collected and transmitted to medical establishments in real time. There is an increasing number of health software applications, both on mobile and desktop computers, that help people monitor and improve their health condition, with or without the use of specific devices (e.g. dietary advisors, fitness applications, applications for diagnosis of health status and diseases). E-health monitoring devices can be classified as crowdsensing applications, according to the categorization in D1.1.

Personalized monitoring devices are also a cornerstone of the EU eHealth policy and research[13]: Solutions based on wearable, portable or implantable systems offer the means to follow patients’

[12] http://europa.eu/rapid/press-release_MEMO-12-959_en.htm
[13] http://ec.europa.eu/information_society/doc/factsheets/009-ehealth-en.pdf

health outside traditional care institutions, thus enabling them to live a more normal life, whilst facilitating efficient management of diseases and early diagnosis of symptoms from a distance.

In terms of the different layers and dimensions of HMNs as defined in D2.2, we have:

Human agencies: Patients provide health information that is included in electronic health records. They can access this information, and manage how it is used together with health professionals. In the handling of eHealth records, the patient is regarded as an active partner in his/her treatment by accessing, adding, and managing health-related data, thereby supporting care (Ball, Smith, & Bakalar, 2007). In addition, patients can use telemedicine applications to remotely communicate with their practitioner, or use wearable devices to monitor their health. On a larger scale, they use computer programs, and particularly mobile applications for monitoring and diagnosing health issues, as well as following a certain diet or fitness program. There is a huge amount of patients and health professionals using more and more such eHealth tools (see Figure 1).

Health professionals/practitioners manage the tools and services for diagnosis, treatment, monitoring and management of health situation of the patients.

In an eHealth HMN, human input may be active, as when a patient fills information needed in an EHR, or passive, as in a monitoring application with wearable devices, where the human agent provides the input to the machine passively, through the physiological actions of the human body.

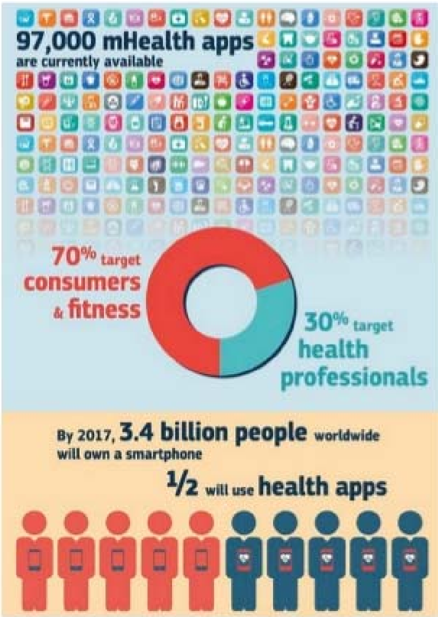

Figure 1: eHealth Infographic[14]

Machine agency: Machines in eHealth sector are apps, wearable technologies, medical devices, mobile devices (termed as mobile health or mHealth), etc. The machine agency is very important in this

[14] https://ec.europa.eu/digital-single-market/en/news/mhealth-what-it-infographic

domain, since the services need to be accurate with no or limited errors. They need to analyse health data quickly, and need to be secured and transparent and also available anytime and anywhere.

The **interactions** between health professionals and patients in eHealth systems are characterized by strong tie strength, for based on the health condition of the patients, he/she may need day to day communication with his/her healthcare doctor. H2M interaction may vary, from a low interaction when the patient views his EHR or checks the proper operation of a wearable device, to a high interaction, when the health professional (or the patient himself) monitors the device's output for assessing the patient's physical condition on a day-to-day basis.

The **size and geographical expansion** of eHealth HMNs differ according to the application. Regarding the size, the number of agents involved in managing EHRs is small and fairly constant, but the data volume can significantly increase, as EHRs permit to collect a huge volume of information about a patient's health, including test results. On the other hand, the size in terms of human agents can be very large for e-monitoring applications, as a single server may communicate with thousands of wearable devices.

Regarding the geographical expansion, in most of the cases telemedicine applications are static applications between two endpoints; but these endpoints may be located very far from one another (e.g. doctors performing tele-surgeries to patients abroad). In case of e-monitoring applications with wearable devices, the patient may be free to move within some area, usually inside the home where continuous connectivity can be provided easily. However, different technologies can be combined to provide more movement, such as combining different access technologies (WiFi inside the home or cellular networks outside) along with data transmission techniques and synchronization methods that allow continuous monitoring even in cases of intermittent connectivity. Finally, EHRs are meant to be used at least within the country, but also between countries.

4.2.2 Stakeholders involved in eHealth

In eHealth, stakeholders involve:

- **Policy makers**: e.g. national ministries, EU administrations.
- **Health professionals**: both in-hospital (doctors, nurses, administrative) and out of hospital professionals (e.g. family doctor).
- **Patients and users groups**: individuals, as well as groups representing patients, primarily interested in improving the quality of user experience, privacy and confidentiality issues.
- **IT experts for eHealth**: Companies developing eHealth applications, telemedicine systems, monitoring devices.
- **Research experts**: computer scientists and engineers, as well as researchers involved in patient management, care management and management of patient information.

National health ministries are typically responsible for protecting and promoting public health through prevention and provision of medical, pharmaceutical and hospital services, following the standards and directions of the EU and World Health Organization (WHO). On European level, the relevant general directorate is DG Health and Food Safety, whose goal is similarly to protect and improve public health, to minimize public health risks for European citizens, and to monitor how the related directions and laws are implemented in each country.

Since the main goal is to find implications of HMNs for policy makers, the latter group constitute the main target of HUMANE. Implications are meant as objectives that should be met by successful HMNs, together with strategies to achieve them, so that they can be adopted in everyday practice. HUMANE intends to engage policy makers, primarily on EU level, from the very start. The roadmap for eHealth will be presented to policy makers in various iterations, and their feedback will be sought in order to align the roadmaps with their requirements and plans, and make them part of future policies.

Health professionals will have the main responsibility in correctly applying eHealth practices. Therefore, it is important to assess their level of readiness to adopt the new technologies, as well as the best way to adopt them. Their engagement is important for determining the status of eHealth services and setting reasonable timeframes between milestones in our roadmap.

The engagement of patients and user groups is most important for ensuring the adoption of eHealth services on a large scale. Our primary goal is to bring out the benefits of the adoption of eHealth services to the broader public, and determine their current familiarity with such services. This can also be helpful in setting reasonable timeframes in the roadmap. In addition, user engagement can help to distinguish levels of manageability that could be applied to eHealth devices and applications, according to the expert level of users, as well as the user privacy requirements.

IT experts can provide feedback on the current capabilities and limitations of eHealth systems, their current penetration in the market and problems that hinder their widespread adoption. Researchers can provide more details on problems regarding service scalability, availability, privacy and security. However, they can also receive information about the high-level objectives set in the roadmaps, and where the focus of future research is likely to be.

Apart from the individual feedback of each of the above groups, their interaction is very important and can contribute to the efficacy of the roadmap. Natural interactions exist between some of the groups (e.g. policy makers and health professionals, health professionals and patient groups, IT experts and researchers), which means that there already exist ties and a common basis for communication. HUMANE aims to profit from such ties and organize interactive workshops, where these groups can work together for providing ideas and directions for the roadmap, and participate in deciding priorities and strategies.

4.2.3 Specific challenges and high-level objectives of HMNs used in eHealth

From a technical viewpoint, the high-level objectives are to construct eHealth systems that are scalable, have a high degree of availability, are invulnerable to security threats and attacks, and inspire trust to their users that their personal data are used only by certified people and only for a predefined purpose. Generally, privacy also has a significant legal component, which involves the establishment of legal rules and procedures for the handling of such data, and punishments or remedies for their violation. However, we regard it as a technical challenge to build the access, management and accountability mechanisms that can provide for the privacy of eHealth data, and detect privacy breaches when they occur. The patients or health professionals (many of which are usually resistant to new methods of clinical practice) may be reluctant to use eHealth systems even after a safe and privacy-enabling environment is constructed. Therefore, additional methods such as advertisement campaigns and pilot programs would be required to overcome the initial resistance. Other non-technical objectives are to ensure and devise appropriate business models so that the usage cost remains low and eHealth systems can be adopted by all patients, regardless of their economic capabilities. Additionally, large-scale clinical studies should be carried out in order to analyze the behavior of both humans and machine agents in a realistic environment.

Below we have a categorization into technical and non-technical challenges and provide more details. Most of the non-technical challenges are also highlighted as barriers to deployment of eHealth solutions in the EU eHealth Action Plan 2012-2020[15]. We remark that health-monitoring applications share many of the challenges identified for crowdsensing in D1.1, such as effective privacy protecting measures, or processing and analyzing the collected data. A notable difference, however, is that usually there is no difficulty in providing incentives for use, as the interest for monitoring and improving one's health usually provides sufficient incentive.

Technical challenges:

- ***Scalability***: eHealth systems should be scalable in order to manage huge amounts of health data (such as EHRs, or data from monitoring devices).
- ***Availability***: eHealth systems should be available continuously because any unavailability of computing and on-line connectivity may produce a major risk to patients' health. This particularly concerns remote monitoring systems, which should be robust to device or link failures.
- ***Data security***: The health data should be secured and protected prohibiting vulnerability. There is lack of a standard code of generally accepted practices and protocols for eHealth services, in extension to those used for data in general. In fact, many of the sensor networks applications in the healthcare are heavily relied on technologies that can pose security threats like eavesdropping and denial of service.
- ***Privacy and confidentiality***: Even if the eHealth system uses advanced security algorithms, and data from patients or individuals are obtained with the consent of the person, misuse or privacy concerns may emerge. For example, in using sensor devices, people would fear that such devices may be used for monitoring and tracking individuals by government agencies or other private organizations (e.g. insurance firms checking client health) (Al Ameen, Liu, & Kwak, 2012). It is hence necessary to apply consistent rules in the EU for the management of medical information, including patient data.
- ***Standardization and interoperation*** between different devices is necessary for widespread usage, within and across national boundaries.

[15] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52012DC0736

<u>Non-technical challenges</u>:

- ***Cost***: One of the goals of eHealth systems is to reduce healthcare costs by promoting out-of-hospital treatment and patient engagement. However, hardware and software in such networks should not have a high cost, in order to be widely adopted. Thus, the cost-effectiveness of such systems needs to be further assessed.
- ***Business models*** have to be derived, that ensure the future sustainability of such systems, in particular for the systems or devices that are used by patients themselves, in order to ensure the use of high-quality products at low cost.
- ***Clinical validation***: Apart from electronic health records, other eHealth systems are not widely used in eHealth practice. Clinical trials should cover the whole range of methods and tools on eHealth, including systems and devices for self-management of health.
- ***Legal framework***: There is a lack of legal clarity about the status of health and wellbeing applications, which are flourishing, especially in the mobile market. Consequently, eHealth application manufacturers may not be fully aware of the legal norms their applications must adhere to, or their responsibilities towards the end users.
- ***Increase trust and mitigate resistance from the patients and healthcare providers***: Even after a safe and privacy-enabling environment has been constructed, still these groups may be resistant and not willing to participate in eHealth systems. The causes of such resistance may lie in usability, cost, fear for their safety (e.g. electromagnetic radiation of wearable devices), or for the handling of personal data. Addressing this challenge is linked closely to improving security mechanisms and ensuring the privacy and confidentiality of personal medical data, which constitute technical challenges, as previously described. In many cases, advertisement campaigns or pilot programs for specific areas and users can be beneficial to increase knowledge and awareness, required to encourage the usage of eHealth systems.

In Table 3 we present a mapping of challenges to the relevant stakeholders.

Table 3: Challenges for eHealth as they relate to specific stakeholders

	Policy makers	Health professionals	Patients and user groups	IT experts	Research experts
Scalability				X	X
Availability		X	X	X	X
Data security				X	X
Privacy and confidentiality			X	X	X
Standardization and interoperation	X			X	X
Cost	X	X	X		
Business models	X				

	Policy makers	Health professionals	Patients and user groups	IT experts	Research experts
Clinical validation					X
Resistance	X	X	X		

4.2.4 Policy background, current initiatives and future policies in eHealth

The EC adopts its Digital Single Market strategy for Europe, which aims to make the EU's single market freedoms "go digital" and boost growth and jobs in the EU. The strategy is deigned to prompt eHealth interoperability and standards in the EU, for the benefit of patients, health professionals, and health systems and industry.

With the mobile health market evolving rapidly, EU health policy is addressing eHealth and mHealth issues within its areas of competence:

- A first action plan in 2004 focused on electronic prescriptions and computerised health records. This e-health Action Plan anticipated the creation of a European eHealth area, with free patient mobility and empowerment of the citizen through eHealth services. An important part of the plan was a Roadmap for Interoperability of eHealth Systems Programme (RIDE)[16], which would develop community-wide recommendations for fostering eHealth technologies that share a common "vocabulary" or operating platform. Interoperability was identified as both a pre-requisite and a facilitator for eHealth deployment. The roadmap identified four pillars of Health interoperability: Electronic identification; Technical interoperability; Semantic interoperability and legal and regulatory interoperability.
- In 2012, after a public consultation, the Commission adopted a second plan for 2012-2020, following the adoption of the directive on patient's right in cross-border healthcare. The eHealth Network established in 2012 has already finalised several reports to increase the uptake of eHealth in the European Union, and the European Parliament has supported the Commission's plan. According to this plan, one of the barriers to development of eHealth is the lack of clarity on legal and other issues around mobile health ("mHealth") and "health & wellbeing applications" and about the role that network operators, equipment suppliers, software developers and healthcare professionals could play in the value chain for mobile health.
- In April 2014, DG CONNECT's Green Paper consultation on mobile health explored questions of privacy, patient safety, legal frameworks and cost-effectiveness. Based on the answers, the Commission has discussed potential policy actions with stakeholders throughout 2015.

In a policy and research fact sheet about eHealth[17], issued in 2011, it was mentioned that the ICT for eHealth program of the EC would focus on the interoperability of health information systems, on clarifying the legal framework for telemedicine and on supporting solutions based on wearable,

---

[16] http://www.ehgi.eu/Download/European%20eHealth%20Interoperability%20Roadmap%20[CALLIOPE%20-%20published%20by%20DG%20INFSO].pdf
[17] http://ec.europa.eu/information_society/doc/factsheets/009-ehealth-en.pdf

portable or implantable systems. A special emphasis would also be put on the protection of personal data and on regulatory issues to ensure that the eHealth can fully benefit from the Internal Market ensuring high quality, transparency and better prices for customers. A more recent publication of the EC DG for Health and Consumers discusses the use of Big Data in public health policy and research[18]. The size and heterogeneity of the data being collected was identified as a major challenge. In addition, the report emphasized the lack of cross-border coordination and technology integration, which calls for standards to facilitate interoperability among the components of the Big Data value chain.

Finally, under the Horizon2020 programme[19], the EU plans to invest more than €2 Billion on projects related to Health, Demographic Change and Wellbeing. Amongst the goals of the programme are to improve our ability to monitor health and to prevent, detect, treat and manage disease, as well as test and demonstrate new models and tools for health and care delivery. The 2014-2015 period included calls for ICT solutions for assisted living environments, self-management of health and disease and patient-empowerment through ICT, decision support systems for self-management, innovation in organizational and business models for service delivery, as well as standardization and interoperability of ICT platforms, methods and services for eHealth. For the 2015-2016 period, the above topics were also included; in addition there were specific calls for scaling up of ICT solutions for active and healthy ageing, as well as on Big Data methods supporting public health policies. Related calls should also address topics about ownership of data, data protection/privacy, liability and consumer protection.

Key facts and statistics from the WHO[20]

93% of Member States (42 countries) have made public funding available for eHealth programmes, showing the strong commitment of governments for further development in the sector.

81% of Member States (35 countries) report that their health care organizations are using social media to promote health messages as part of health campaigns. 91% (40 countries) report that individuals and communities use social media to learn about health issues. These data demonstrate both strong uptake of social media and interest in its potential as a communication medium for both patients and professionals. Yet, 81% of Member States report having no national policy to govern the use of social media in health care, leaving the use of social media informal and unregulated.

80% of Member States have legislation to protect the privacy of individual health-related data in electronic health records – an increase of nearly 30% since 2009. This indicates significant progress in adopting electronic health records responsibly.

73% of Member States (33 countries) do not have an entity that is responsible for the regulatory oversight of mobile health apps for quality, safety and reliability, despite widespread use of such technology. This presents a potential risk for countries and is an area in need of incentives, guidance and oversight.

[18] http://ec.europa.eu/health/ehealth/docs/ev_20141118_co07b_en.pdf
[19] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/health-demographic-change-and-wellbeing#Article
[20] http://www.euro.who.int/en/media-centre/sections/press-releases/2016/03/e-health-when,-not-if

38% of Member States (17 countries) have yet to establish a dedicated telehealth policy or strategy. Given the considerable increase in telehealth initiatives in Europe, this area requires more dedicated focus by governments to ensure a solid foundation for its continued growth.

Within the EU, Denmark, Finland, Sweden and the UK offer the best market condition for mHealth to flourish based on eHealth adoption, regulatory framework, level of digitalization, practitioners' perspective, and market size[21]. Germany and France, despite being huge markets, are hampered by lack of regulations, digitalization and adoption (by consumer and practitioners) diminishing and complicating their market potential and growth prospects.

4.2.5 Opportunities for policy interventions in eHealth

Notable opportunities for policy interventions in the eHealth area are:

- **R&I actions on eHealth**: Almost all of the challenges and objectives we identified in 4.2.3 have been included in calls relative to the Horizon2020 programme on Health, Demographic Change and Wellbeing. From the analysis of existing calls for the 2014-2015[22] and 2016-2017 periods[23] , it seems that small emphasis has been given on privacy and security of eHealth services so far; as this has been mainly a requirement of system design rather than a stand-alone topic. Overall, the research and innovation policy on eHealth should review the outcomes of the research so far and pursue outstanding or insufficiently addressed goals.
- **Rules for the management of medical data:** Medical data is treated like personal data and is covered by the Data Protection Directive 95/46/EC. This directive recognizes the need of health professionals to process health-related data of individuals even without explicit consent, and leaves it up to the health agencies in each country to provide safeguards that protect the fundamental rights and privacy of individuals. This general approach creates uncertainty regarding the access to and sharing of medical data that is occuring without knowledge of the patient. This is exacerbated by the use of wearable devices that can transmit health-related data continuously. Big data technologies provide the means for distributed processing, storage and management of large volumes of data; however there needs to be clear legislation governing access to such data and empowering the patients to take control of data that concerns them. There must be clarity regarding the utilisation of personal data produced by eHealth applications. In addition, accountability in case of misuse should be provided. There is also a need for different levels of detail in data records, from the detailed history of treatment and results required by doctors, to anonymized statistics used to inform public policies.
- **Policy for regulating eHealth applications:** Many eHealth applications are used in the market without recommendation or certification by an established health organization. In this case, many applications could be potentially dangerous if no verified methodology is followed. There is

[21] http://research2guidance.com/r2g/research2guidance-EU-Country-mHealth-App-Market-Ranking-2015.pdf
[22] http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-health_en.pdf
[23] http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-health_en.pdf

currently a lack of legislation governing the marketing and usage of such applications, which operate at the sidelines of medical practice.

- **Policy for QoS-enabled medical services:** The current best-effort Internet services may not satisfy the stingent throughput and delay requirements of telemedicine applications, especially the ones that are critical for the life of the patient (e.g. telesurgery). At the same time, the cost to build private infrastructures that are unaffected by congestion problems in the public Internet is prohibiting the wide use of such practices. Hence there is a clear need to provide QoS-enabled services for medical applications at low cost, ensuring high availability and efficiency of critical applications such as telemedicine and real-time monitoring operations. The recent EU Regulation 2015/2120 protecting open access to the Internet allows the creation of services with enhanced quality, but without undermining the quality of Internet access for the remaining services. This poses a difficult problem, and further interventions may be required by EU bodies and regulatory authorities.

4.3 Citizen participation

4.3.1 Topic description

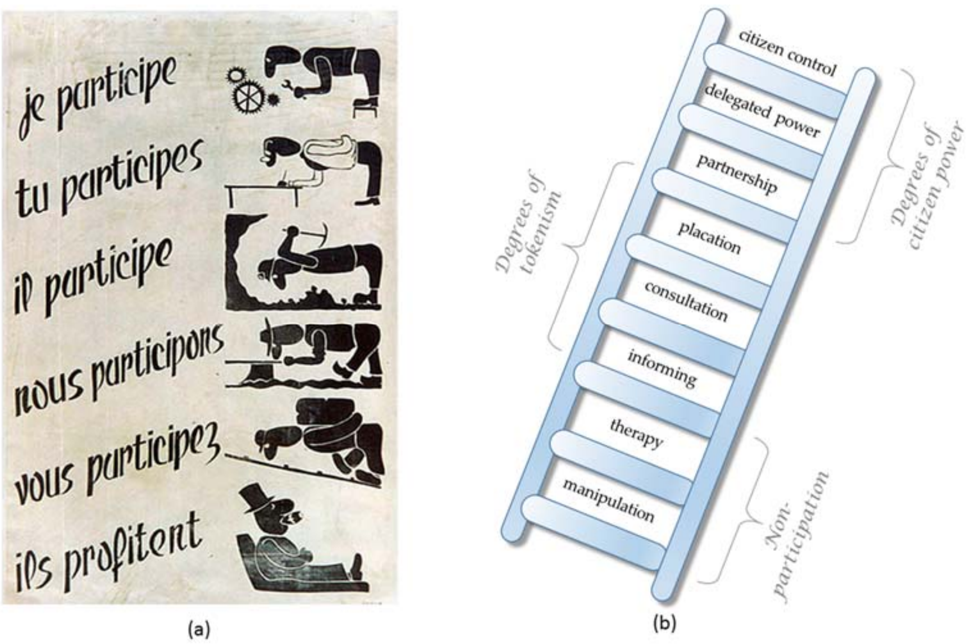

Figure 2: (a) the 1968 satirical representation of participation by the *Atelier populaire* (b) The Ladder of Citizen Participation (Arnstein, 1969)

The concept of *citizen participation* is not without controversy. As far back as Arnstein (1969), it was already well-established that there was something sinister and underhand about encouraging participation, summarised in a satirical poster from the *Atelier populaire de l'ex-École des beaux-arts*[24]

[24] The accompanying image has been released into the Public Domain by the *Bibliothèque nationale de France*

(Figure 2 (a)). Arnstein elaborates by developing a ladder of participation running from non-participation associated with 'manipulation', through tokenism, to citizen power with 'partnership, delegated power and citizen control' (Figure 2 (b)). Her more nuanced interpretation has coloured much of the theoretical work in the area since, and at the very least provides a basis upon which to evaluate participatory networks.

Across the human-machine networks that we have reviewed and those we have studied in some detail, it is apparent that Arnstein has a point. Social networks, for instance, provide some form of 'therapeutic' outlet for many participants in developing and presenting a public persona to their would-be peers, whilst the more recent commercialisation of such networks may be said to 'manipulate' subscribers. Such manipulation includes recommender systems which seek to predict and influence potential future purchase decisions on the basis of what a consumer has already bought, and by highlighting what other, allegedly similar, consumers have purchased (Adomavicius & Tuzhilin, 2005). This manipulation may, however, be more insidious whereby search-engine results are filtered in accordance with monitored online activity (Fortunato, Flammini, Menczer, & Vespignani, 2006; Meiss, Menczer, Fortunato, Flammini, & Vespignani, 2008), thus presenting a consumer with only those results which they might have expected, or which align with a commercial or political agenda. These are at the level of *non-participation* according to Arnstein (*op.cit.*). Yet as the Arab Spring as well as the London riots in 2011 demonstrate, there is significantly more potential for open exchange and inter-citizen interaction within such networks, which would conform to some extent with Arnstein's first level of participation through partnership. We note, however, that as social machines supporting social networking attract marketing and retail activity, for example through advertising alongside popular YouTube videos or targeted advertising derived from automated analysis of FaceBook exchanges, so the networks start to take on the characteristics of more complex socio-technical systems or actor networks. Nonetheless, these networks cannot be considered to be more than participatory, in the sense that they do not allow the users to climb Arnstein's ladder to achieve any level of delegated power or control. Where eDemocracy has been lauded in community, local or national contexts, the reality has been merely at the level of participation, where websites have been hosted to gather comment, or opinion has been garnered and analysed for sentiment drawn from twitter or FaceBook discussion. Whilst these might create the opportunity for citizens to feel that they are communicating with those in government, the reality is that the input from citizens has little direct effect on government decision making or policy. Influence is at best indirect, through coordinated direct action, such as seen in the grass-roots exchanges in riots or revolution, or through the combined weight of negative opinion circulating on social media and often amplified by national and international media outlets. But even in this case, there is a case to be made that this is in fact manipulation through social media of the people subscribing to it, rather than the users of social media driving opinion for themselves. In order that citizen participation moves up Arnstein's ladder to the highest rungs of delegated power and ultimately control, it will be necessary for those that currently exercise power to permit its delegation to the crowd, and for the crowd to be sufficiently representative of the population as a whole. This will necessitate the inclusion of checks and controls on the networked behaviour, exercised through the existence of machine agents within the network implementing moderation in a non-partisan way, and controlling the natural desire of individuals to dominate and direct those around them. Thus it can be seen that for citizen participation through networks to escalate up Arnstein's ladder, then those networks need to exhibit all the characteristics of human-machine networks, in which both the human and machine actors exhibit agency.

In this section, we set out some of the characteristics of these networks and the ecosystem around them.

At one level, existing social networks provide an interesting foundation for enabling citizen participation to some degree. Users are encouraged to share experiences and opinions, which helps develop the socio-technical behaviours to share, discuss, pass comment and provide support to each other, an essential basic activity that allows other, more specific network purposes to be enabled. Within HUMANE, all of the trial networks we have studied depend upon human participation, although, not all of the networks might traditionally be regarded in that way. It is important therefore to begin to identify some of the characteristics shared by these networks that can be considered to be common to HMNs which support citizen participation.

In terms of the different layers and dimensions of HMNs as defined in D2.2, we have:

Machine agency: for citizen participation, machine agents are commonly ICT platforms, which facilitate discussion, negotiation and content sharing. Social networks are an obvious entry point, but also knowledge creation systems fall into this category. We note that:

> "*Enhanced communication has evolved hand in hand with enhanced citizen participation. Both have been increasingly integrated into policy planning, budgeting, and government processes more generally. Citizens increasingly are making the leap from policy awareness to demands for accountability*." (Mozammel, M., 2011)

Increased access to open data sources, for both policy makers, intermediaries such as NGOs and citizens[25] means that there is an increasing involvement of machine agents performing such functions as data mining, information filtering and fusion, which permit an increased range of action for the policy makers, but also permits greater freedom of action and influence for connected citizens. As such, whilst machine agency has tended to be low in the past, developing networks of citizens and policy makers are increasingly becoming reliant on greater levels of machine agency. Thus, both commercial as well as governmental exploitation of online participation involves greater levels of machine intervention, with algorithms typically deployed to analyse online activity to 'profile' user interest and spending patterns on the one hand, or review online exchanges for grassroot sentiment and feeling about a wide range of issues on the other. ***Machine agency has now increased***, without users being fully aware of this change. The human agents in the network may well believe themselves simply engaged with a social machine, whereas in reality they may be dealing with bots and with other intelligent agents that are collecting information on behalf of other agencies. In the future we can anticipate a situation in which machine agency is more explicit, meaning that citizen participation becomes much more a *partnership* in Arnstein's terms. The greater level of perceived connection and

[25] http://www.mckinsey.com/business-functions/business-technology/our-insights/open-data-unlocking-innovation-and-performance-with-liquid-information

access enabled by active machine agents in the network will encourage greater engagement between citizens and government or commercial agencies through, for example, technology-mediated opinion sharing or information exchange.

Human agency: current models of citizen participation are based around the provision of official information to citizens via dedicated websites or social media communication. Engagement by the citizens with those in government or local administrations is conducted at a distance, through comments on websites, email communication to generic inboxes or other off-line methods. Increasingly, also, citizens are communicating amongst themselves using Twitter, Facebook or community networks (e.g. fixmystreet[26], streetlife[27] in the UK). This activity represents an increasing level of human agency, but is presently focused on community engagement between peers in contrast to the interaction with governance that citizen participation is often taken to demand. However, increasing machine agency, in the form of crawlers tracking and analysing community discussion and sentiment, for example, allows greater representation of citizens' views and opinions to policy makers and other government representatives. This does not immediately change the behaviour of ordinary citizens, but in the longer term, as realization of the inferred information channel from citizen to government becomes more obvious so citizen behaviour is likely to evolve to reflect the impact that their discussion and comment can have on policy decisions. It seems unlikely that, in the short to medium term at least, social structure will change to allow for movement up the Arnstein ladder to delegated power. Instead, it is more likely that human agency will expand from agency only in the H-H interaction to encompass community agency (that is higher agency of related or connected groups of people) which are able, through coordinated action, to influence governmental and policy behaviour.

Interactions: As noted above, H-H tie strength can be high in citizen participation networks between peers, but can be low between the citizens and other human groups such as government and policy makers. These connections are currently mediated by simple H-M connections, which are likely to become more active as the machine agents connecting these different groups exhibit higher agency. This is inevitable, since there are very many more citizens than there are government contact points, and so management and aggregation of their input to the policy process must be performed automatically in order for it to be effective. Humans naturally form groups of those with similar interests, creating stronger tie strength within such groups (which may be dispersed across geographical or demographic lines, depending upon their common interest) and weaker ties with other groups (that is the out groups), extending to rather weak ties with government groups that are mediated and aggregated via machine agents.

Network Extent: A citizen participation network can be considered to comprise several 'scales' at which it operates, and the overall network is a complex mix of sub-networks having their own characteristics. Consider a network in which citizen participation is conducted at local and national levels. As discussed earlier, the citizens themselves form common interest groups, common

[26] https://www.fixmystreet.com/
[27] https://www.streetlife.com/

demographic groups and common location groups, within which they exchange information and opinion and from which they seek to influence policy. These groups may have limited geographical extent (in the case of a local interest group such as streetwise[28]) or a very broad geographical extent in the case of common interest groups (such as sports or motoring networks) where members of the 'in-group' may be located anywhere in the world. These sub-groups will often form 'bottom-up' networks and will grow according to the dynamics of an evolving, low regulation network. However, the government groups with which the citizen groups hope to engage are also organised as networks, but these are much more structured and hierarchical and often exhibit top-down characteristics. They are of limited geographical extent, and as we have seen, they tend not to have direct engagement with the citizen groups, but rather interact via machine intermediaries.

We might also consider other networks which form part of this group – for example business networks which are often established on regional bases, and which have the intention of direct lobbying of government, but have no direct link with private citizens or their networks. Finally we have NGOs, which have links with both government, via direct lobbying, and citizens via online or machine intermediaries, although NGOs can be considered as actors rather than sub-networks.

4.3.2 Stakeholders involved in citizen participation

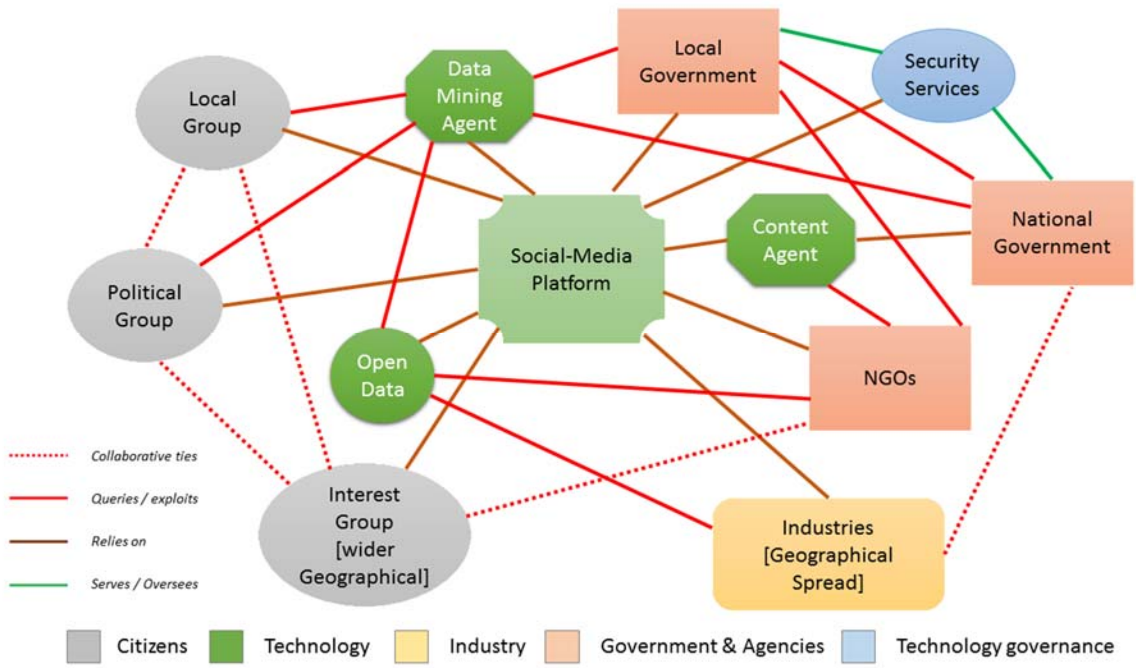

Figure 3: Main stakeholders involved in Citizen Participation HMNs

As we have seen above, the stakeholders in citizen participation networks tend to be arranged as sub-networks comprising related stakeholders which interact in a variety of ways. At the grass-roots level, networks of individuals are emergent, exhibiting common goals and aspirations, although networks may also be developed under the auspices of a lobby-based NGO trying to build public interest

[28] https://www.streetwise.net/

coherence in order to support its lobbying activities. Government, government researchers, policy makers and politicians are clearly also stakeholders, each with their own agendas and ambitions, and each using various on-line techniques to interact in some way with other stakeholders. We can add to this mix those who devise and implement the platforms and machine agents that mediate the interaction. Governments maintain IT departments whose role is to ensure that internal communications and external communications are maintained and managed, and the quality, accessibility and style of these platforms will determine the effectiveness of the communication.

In the past there has been very little direct engagement between these different stakeholders, however the advent of machine agency within networks has the potential to support engagement in a variety of ways. There are many emerging platforms that bring together individuals with common interests, thus amplifying their voice, and in parallel there are machine analytics and tracking agents that monitor this voice and can report to government and policy makers such things as the sentiment or key interests of groups of individuals.

Table 4 relates stakeholders to the identified challenges for citizen participation networks:

Table 4: Challenges for citizen participation as they relate to specific stakeholders

	Local and National Government	Citizen Groups	NGOs	Industry	Security Services
Motivation	X	X			
Trust & Security	X	X	X	X	X
Control	X			X	
Accessibility	X	X			
Transparency	X	X	X	X	
Accountability	X			X	X
Regulation/legislation	X	X	X	X	X
Subversion	X			X	X

4.3.3 Specific challenges and high-level objectives of HMNs used in citizen participation

Different actors within citizen participation networks have different objectives. The individual citizens want to make their voice heard. They want to engage with like-minded individuals and create a unified voice to increase their lobbying power with local or national government. On the other hand, government and politicians have a number of conflicting objectives. They are maintained in power through the exercise of democratic choice by ordinary citizens through the mechanism of periodic voting, they need therefore to keep citizens on-side and supportive, but they also have broader goals of meeting financial and social targets which may disadvantage some members of the population in favour of others, leading to political conflicts such as the benefit to industry versus benefits to the population or the environment. From the point of view of the citizen participation network of which they are all a part, there are a number of 'meta-layers' of behaviour that need to be considered.

- **Motivation**: In order to engage with, and remain engaged with, a network, the various human parties need to be motivated to continue that engagement. Motivation is built upon reward or benefit, which in citizen participation networks is based upon the sense of achievement and recognition. There is therefore a challenge for governments and policy makers, who as we have observed do not have a direct connection with individual citizens via the network, to demonstrate responsiveness to the contribution they make. There needs to be a feedback path, possibly mediated by the platform or machine agency operating on it, from the governmental to the individual level.
- **Trust**: It is far easier to lose trust than to gain it. There are many connections within a citizen participation network where trust plays an important role. In general, citizens trust other citizens in their network who express similar opinions to themselves, and they may display more or less trust in the politicians who run government, although it has been noted elsewhere (Acquisti, 2012), (Dinev, Hart, & Mullen, 2008) that people are more prepared to share personal data with a supermarket chain than with the government. There also needs to be a high level of trust in the intermediating machine components that aggregate and present citizen opinion, yet the algorithms on which they are based can often be seen as arcane and incomprehensible. The role that trust plays in these networks needs to be better understood and levels of trust increased through better communication of intent and function.
- **Control**: The question of who or what exercises control in a network can impact perceptions of trust, and as a consequence reduce the motivation for engagement. An analysis of the interaction between the various actors involved in a network needs to include a definition of the distribution of control of the network behaviour between actors, and the perception of the human actors of how this control is exercised.
- **Transparency**: In a citizen participation network there are many opportunities for information to be withheld or obfuscated. Lack of transparency is caused by unbalanced control, leading to a loss of trust and ultimately loss of motivation for participation. Thus transparency is an essential component of a healthy and effective network, and a significant challenge in the design and operation of a network is in ensuring transparency and ensuring that the transparency is appreciated by all actors.
- **Accountability**: As we have seen, citizen participation networks are characterised by sub-networks having different network functionalities. Accountability is often an abstract concept, particularly where the network has developed bottom-up without any clear overall controlling entity. If decisions are made, for example by policy makers or government, then it needs to be clear on what basis those decisions have been made, and by whom they have been authorised. This level of accountability is necessary in order to build and retain trust by actors in the network.
- **'Dark Web' / Civil unrest / Hypocrisy**: There are other, more subversive influences that can undermine the operation of a citizen participation network, or undesirable activities that can be

pursued using the facilities that the open network offers. Criminal activity, conducted over the 'dark web' can lead to exploitation of vulnerable citizens through various methods of deception. These are criminal activities, and as such need to be tracked, identified and prosecuted by the traditional law enforcement agencies. Since by its nature citizen participation networks have international connectivity, close communication and information exchange is needed between law enforcement agencies across national boundaries. The law enforcement agencies and security agencies are stakeholders, or actors, that should be considered as essential actors within these networks.

The positive aspects of citizen participation are shadowed by the other, subversive activities that can be undertaken and pursued by those that wish to pursue or foment unrest, and the distribution of false or misleading information is a part of that activity. A foil to this activity is the use of the network to disseminate counter information, however the value of doing this is undermined if those providing the information do not have the trust of the public. Unfortunately, this can be the case if the source is politicians or police agencies, which have a reputation for manipulation of facts, and in consequence do not engender sufficient trust amongst ordinary citizens who are using the network. We can therefore see the value of trust, and trusted behaviour in the network and can also see that politicians, policy makers and public information agencies are stakeholders for whom creating and preserving trust is important.

4.3.4 Policy background, current initiatives and future policies in citizen participation

One of the guiding principles of the digital agenda is increasing citizen participation in the process of government and policy making, as enunciated by Andrus Ansip in the recent European eGovernment Action plan for 2016-2020:

> *"The industrial revolution of our time is digital. … As companies aim to scale up across the Single Market, public e-services should also meet today's needs: be digital, open and cross-border by design. The EU is the right scale for the digital times."* Andrus Ansip, Vice-President for the Digital Single Market; April, 2016[29]

This can only be achieved by developing the internet-enabled networks that can be used for bringing together groups of citizens to express their views, and providing the connection between them and the representatives of government and policy with whom they need to communicate. Individual citizens do not have a strong voice when it comes to democracy – that voice is heard most strongly when citizens are able to share common concerns, and present them to elected authority as a group. This is what digital citizens are enabled to do. In the past, democracy has relied on the ballot box – the periodic exercise of collective votes based on the combination of a number of stated policies forming a political manifesto, and emotional perceptions of the personalities standing for election to

[29] EU eGovernment Action Plan 2016-2020 "Accelerating the digital transformation of government". Available online: https://ec.europa.eu/digital-single-market/en/news/communication-eu-egovernment-action-plan-2016-2020-accelerating-digital-transformation

Parliament. There are many disadvantages to this system, not least the limited number of opportunities for citizens to express their opinion, and the fact that elections are fought on a number of different policy proposals, not all of which may be supported by each voter. Once elected, a government is free to interpret the will of the electorate on the assumption that the majority has endorsed all of their policies. There are many other issues, such as the percentage of the electorate voting, and their demographic makeup.

eDemocracy allows citizens to express their collective opinion on single issues, and to express their opinion more often than in the past, although as we have seen in the recent Brexit vote in the UK, this can lead to unexpected results, especially when combined with traditional approaches to campaigning and influencing the electorate.

4.3.5 Opportunities for policy interventions in citizen participation

The main interventions necessary in the evolution of citizen participation networks fall into the categories of control and limitation on the one hand, and support and evolution on the other. The principle aspect of such a network which will limit the involvement of citizens, and hence growth of the network, is one of trust. In order to use the network, citizents need to have confidence in the security of the network, they need to be willing to trust the technology, they need to trust the governmental departments which it represents, they must have confidence in the security agencies policing the network and they need to have a belief in the network that their voice will be heard by those in authority.

In order for the network to grow in size and usefulness it needs to be accessible to all demographics, religious and social groups. It needs to prevent exploitation by commercial, political or religious groups, ensuring it remains non-partisan and open and there needs to be a feedback mechanism to citizen particpants confirming that their voice is being heard. This will be a difficult balance to achieve, and at times will appear impossible to reconcile. Ideally, management of the citizen participation network would be achieved by regulation rather than legislation, with confidence being generated by positive response to citizen involvement by government representatives. It will be important for open data to be available to all in the network, which will encourage the development of applications exploiting data to provide additional services, but for controls to be in place which restrict the ability for commercial, political or criminal actors to mine personal data for their own ends, which would clearly undermine trust.

Regulation or government intervention may be necessary in order to ensure that currently under-represented demographics, such as the elderly, socially disadvantaged, minority groups such as LGBT or those inhibited by gender stereotypes are supported, or even encouraged, to be part of the citizen participation network. This is important, since one evolution of the citizen participation network will be towards greater social inclusion in the democratic process, and it is incumbent on governments to ensure that all citizens have equal access to eDemocracy networks. Moreover, it will be important to ensure that the aggregated contribution of citizen and special interest groups is recognised in policy decision making, to avoid the loss of trust that many participants would feel if they considered that their views were not being recognised.

There is an opportunity to incorporate many networks into the citizen participation ecosphere, with the proviso that regulation and monitoring will be enssential to ensure that privacy and ethical use of information are maintained, such as between financial, health or social interactions, and to track and control criminal activity, coercion and political fraud. These are, ultimately, management approaches which will engender and maintain trust in the growing citizen participation network and ensure it achieves its goal of transferring power and influence to all citizens.

4.4 Telework

4.4.1 Topic description

Telework includes methods, platforms and systems for working and cooperating with other workers from a distant location, via the use of ICT technologies.

ICT technologies, in particular email, access to the Internet, web conference tools, and remote access to the workplace network have given new dynamics to the concept of teleworking and have enabled its widespread adoption – at least for some days per month for several countries – or even the creation of exclusively teleworking jobs (Jackson & Wielen, 1998).

The benefits of teleworking are numerous and well-documented:[30]

- Resolving traffic congestion, reducing pollution and saving energy by decreasing the number of commuters.
- Reducing labour and overhead costs, such as costs for office space and operating/maintenance costs.
- Attracting a wider range of employees,eliminating skill shortages, and offering employment opportunities for the handicapped.
- Increasing work flexibility and reconciling the conflicting demands of work and family.
- Reducing travel costs and fatigue of employees.
- Increasing job satisfaction and employee retention.

Teleworking includes a variety of decentralised work arrangements in addition to work at home. Variation exists amongst teleworkers and homeworkers in terms of, for example, their contractual arrangements, employment status, type of work and work location (Cath Sullivan, 2003). Three types of teleworkers can be discerned (R. Kelly Garrett, 2007):

- Fixed-site teleworkers, whose ICT-supported remote work is primarily at home.
- Flexiworkers, who operate in a combination of office, home and field locations.

[30] Addressing the Challenges Facing the Distributed, 21st Century Business Through Telework. Available online: http://download.microsoft.com/download/D/A/3/DA3F0BAB-40FC-44F9-ACF2-1B1F4E157802/Documents%20for%20refresh/addressing_challenged_facing_distributed.pdf

- Mobile teleworkers emphasizing use of ICTs in field locations (e.g. salesmen traveling around).

Telework relies on technologies such as high speed Internet access, e-mail, VoIP and instant messaging applications, collaborating tools, including web conferencing, and VPNs (Virtual Private Networks), which are almost always used to allow access to corporate resources from outside of their direct network. In addition to VPNs, cloud computing where the user accesses a remote service or application at a distant server via the Internet is starting to be used extensively in teleworking applications. Finally, the use of mobile technologies has also enabled the spread of teleworking, particularly through the use of mobile devices with high computing power and high-rate mobile data networks.

In terms of the different layers and dimensions of HMNs as defined in D2.2, we have:

Human agency: Human agency is high, since humans are the ones that produce the work and communicate it to their colleagues and supervisors by using ICT technologies. In carrying out the work, they may also need to contact third-parties, such as customers, contractors, or the public. Human input of produced is always active, however there may be some information that is provided passively, such as the location of the teleworker, whether or not the teleworker is online, the specific applications or services the teleworker has used, etc.

Machine agency: Machine agency is high, since the ICT equipment acts as a mediator for interaction between teleworkers, fixed-site employees, or a teleworker and third parties. The ICT infrastructure and equipment needs to be fast, reliable and secure, as well as easy to use.

The **interactions** between a teleworker and other human agents may have varying degrees of strength and dependencies, based on the type of work and relations to other teleworkers. A researcher, programmer or consultant working from a distance may have seldom contact to others, or only communicate work deliverables. On the other hand, a teleworker working on customer service from home or teleworkers working from a distance in a collective project will have very frequent interactions. Interactions may also be continuous, as in the case of a conference call, or intermittent, where connectivity is interrupted either necessarily (for example because of teleworker mobility) or on purpose by the teleworker if there are no communication needs.

On the other hand, dependence between a human agent and a machine is strong and interaction is strong and in most cases continuous. Apart from teleworkers on the move (e.g. traveling salesmen), people eligible for teleworking are mostly those conducting deskwork, which can be conducted from a distance using ICT equipment. The strongest tie is between a human agent and the machine in his local environment, but the human agent may also be intensively using distant machines, such as a cloud-computing server.

In terms of the categorization made in D1.1, telework shares some characteristics with public-resource computing, crowdsourcing and mass collaboration. A teleworker may be using his own equipment to work from home, and may share the equipment's resources with other people in his company or organization, from having a shared folder to running a parallel computing experiment. When a high number of teleworkers is involved, teleworking is akin to a form of crowdsourcing, where the human agents are remunerated and undertake tasks that require significant effort. In addition, a network of teleworker can be regarded as a mass collaboration HMN, where human agents use collaborative software for interacting, and creating or modifying content.

There exist yet no official country statistics about telework. The difficulty stems from the fact that there are different applications and degrees of telework in different countries, which may render the results incomparable. In a survey of employees and self-employed workers, conducted by Eurofound in 2005, the overall percentage of workers involved in telework at least 'a quarter of the time' or more in Europe amounted to 7% in 2005 (an increase of 2% in comparison to the year 2000), while the percentage of workers involved in telework 'almost all of the time' was 1.7%.[31] Regarding the sectors of the economy where it is applied, a considerably higher use of telework can be found in real estate, financial intermediation and education. In general, higher educated people are more likely to use telework. Male employees are also more likely to do telework than female workers: according to the same report, on average, about 8.1% of male employees engage in telework, while 5.8% of female employees use this form of work. This rather reflects the distribution of telework among sectors and occupations, as well as the fact that male employees occupy a larger percentage of the jobs requiring high qualifications.

These limited statistics allows us to make some conclusions about other the size and space dimensions of the HMN (see D2.2). Thus, although teleworking only applies to a small percentage of the working force, the trend is increasing, as more and more companies adopt this flexible form of work. In the UK between 2007 and 2012, the number of employees who usually work from home increased by 13% - an increase of almost half a million people, taking the total to over 4 million employees out of a UK workforce of 30 million.[32] The geographical scope also used to be small, usually within the city where the company or organization was based, but now we see more and more teleworkers working for the same company from different cities, as well as from abroad.

4.4.2 Stakeholders involved in telework

Stakeholders involved in telework are:

- **Teleworkers** of various styles and "degrees" (working primarily at home, both at home and at the office, constantly mobile, etc.), each having different requirements and potentially using different tools. Teleworkers are the ones using the technology, therefore their involvement is crucial for accumulating and exploiting user experiences, including problems and difficulties encountered while working from a distance using ICT equipment.
- **Employers** from organizations, the public sector and private companies from different sectors, emphasizing both on sectors where teleworking technologies have been applied very early, such as the telecommunications industry and the retail trade sector, as well as from sectors where the practice of telework is still limited. Of particular importance is also the size of a company, since it

[31] European Foundation for the Improvement of Living and Working Conditions, 2010. Telework in the European Union. Available on line: http://www.eurofound.europa.eu/observatories/eurwork/comparative-information/telework-in-the-european-union
[32] https://en.wikipedia.org/wiki/Telecommuting#Telecommuting_and_telework_statistics

has been observed that smaller corporations are less eager to apply teleworking for their employees. Employers usually have the role of directing and managing telework, and making the detailed teleworking arrangements, which are usually not covered by legislation or collective agreements. The direction of the company or organization usually creates an internal regulation, covering issues such as the time schedules, training and career development, health and safety, equipment and technical support, as well as monitoring and evaluation (see also Section 4.4.4). The employers and managers are also directly responsible for evaluating the efficacy of telework, therefore their contribution is most significant assessing the immediate impact that telework in the company or organisation applying it.

- **Human resource experts,** interested in making best use of the human capital for the development of a company or organisation. This is not only restricted to the task of personnel recruiting, but to all aspects of employment, such as determining the needs of the employees and employers, organisational issues in a work environment, managing employee and employer relations, employee benefits and compensations, dealing with discrimination issues, monitoring performance, promoting motivation, and ensuring conformance to work regulations.
- **Public administration bodies, legislators and policy makers** involved in the issuing of telework regulations and on the monitoring of their application. This also includes statistical bodies, who can provide reliable statistics, both for national use as well as cross-country comparisons.
- **ICT companies**, specialized in telework applications, such as collaboration and web conferencing tools, VPN technologies, secure email and instant messaging applications, synchronization applications, etc.
- **Sociologists, economists and researchers** interested in the social (including the ethics of telework) and economic aspects of telework. Additionally, people working in infrastructure and environmental research, which can help to assess the benefits for the environment and energy savings, as well as the impact on infrastructures (roads, public transportation in a city) and the ramifications that occur for urban management and planning.

Natural interactions occur most frequently between the following stakeholders:

- employees and employers,
- employers and policy makers,
- employers and ICT companies,
- researchers and policy makers.

Throughout the project, we plan to engage all stakeholders, and apart from strengthening the natural interactions, which exist, we will provide channels of communication between all stakeholders. The stakeholder engagement will be pursued primarily through the organisation of joint workshops, where the roadmap for telework will be presented to policy makers in various iterations, and their feedback will be sought in order to align the roadmaps with their requirements and plans, and make them part of future policies.

4.4.3 Specific challenges and high-level objectives of HMNs used in telework

Telework shares challenges with public resource computing, crowdsourcing and mass collaboration. However, there are also specific telework challenges, which we elaborate in the following.

Technical challenges:

- ***Setting up an efficient infrastructure for teleworking***: In telework, employees may use a variety of computing equipment (desktop computers, laptops, tablets, and smartphones) and access technologies (DSL, Cable, Fiber, 3G/4G/5G) with different performance capabilities and access speeds. In addition, they may need to ensure that other users for functions like file sharing, remote program execution, etc. can access their computing resources. Connectivity problems also lead to problems in teleworking, especially for delay-sensitive applications (such as teleconferencing). In addition, accessibility problems may emerge when corporate or user firewalls block access to protocols or applications.
- ***Security***: On a technical level, teleworking may lead to security risks by exploiting vulnerabilities in remote network access to eavesdrop, alter, or modify information.
- ***Scalability of VPNs and other telework technologies***: Regarding the widespread use of VPNs for telework, a related challenge is the effective scaling of such services, since congestion problems may appear when the number of teleworkers in an enterprise increases, or different sites are connected across a single infrastructure. The effective scaling of VPNs will provide less memory consumption, processing power, configuration and better load balancing for large system.[33]
- ***Seamless teleworking from different devices***: Additionally, a number of challenges are related to seamless teleworking from different devices, as well as for people on the move through mobile networking technologies: these include identifying the device of a teleworker and adapting the service interface, synchronizing data, setting up self-organized, ad-hoc cooperation teams, and adapting to an intermittently connected environment for mobile teleworkers properly (Pichler, Hofer, & Leonhartsberger, 2002).
- ***Efficient collaboration environment and tools***: Designing a collaboration environment for telework is also challenging. There exist many platforms and tools for teleworking, from large or smaller manufacturers, license-based or free to use. Currently, different software applications for different purposes exist: email applications, VoIP and instant messaging tools, web conference tools, collaborative editing and file sharing tools, as well as calendar and project management tools. Many platforms are starting to unify different communications needs (e.g. Google offering Gmail, Hangouts, Google drive on a single sign-in platform), but many enterprises may be reluctant to share company information on cloud platforms. Collaboration is also hampered since it is often unknown, on which place the teleworker operates at the moment and which communication tools he could use (depending on the available equipment of the working place like video cameras etc.). Furthermore, there is a lack of advanced collaboration tools for project-based work, in which all

[33] Teleworking scalability Project proposal. Project proposal. Available online: https://www.os3.nl/_media/2013-2014/courses/lia/projects/leendert_anastasios-teleworking_scalability_proposal.pdf

co-teleworkers can see project objectives and progress in real-time, share knowledge and assign or undertake new responsibilities. Most collaborative software products include functionalities for simple project planning and management,[34] however to meet future requirements for supporting project work from a distance more advanced tools are required. A large-scale collaborative platform poses many challenges:

- There are a very large number of collaborators who may not physically meet, and that may change during the course of the project (e.g., some people may leave and others may join). Their skills and expertise must be communicated, or re-discovered as the project progresses.
- Developing, representing and visualizing the progress as it is being made. This includes knowledge management and representation: managing and presenting the already available knowledge, as well as the knowledge created within the project, while respecting privacy and intellectual property rights.
- Building the framework for assisting collaborators for making decisions. This should support both decisions made by large democratic processes (e.g. voting), but also small-scale decisions between, say, two collaborators.
- Building trust relationships for efficient collaboration between people who do not know each other in advance, and may not ever meet.

Further, there are many smaller challenges, from locating and handling communication between a very large number of collaborators, to locating collaborators and creating a secure and user-friendly interface.

Non-technical challenges:

- ***Lack of telework regulations/legislation***: There is a major lack of regulations on teleworking, since it relies mainly on collaborative agreements (see the next section). Among these are regulation for the employment status of teleworkers, the eligibility criteria, the workplace conditions and safety of teleworkers, issues about IPR, and personal privacy. A recent paper (Hynes, 2014) attests that telework remains marginalised in business terms, largely due to the lack of regulation and guidelines essential to legitimise it for employers and employees that wish to work from home. In the absence of legislation, employers retain sole discretionary decision making powers over telework schemes and home working conditions. Indeed, many key decision makers fail to appreciate or recognise the potential benefits that may accrue from telework, which is leading to ad hoc and disorganised arrangements to the detriment of this method of working.
- ***Supervision and performance evaluation of teleworkers, without infringing on their privacy:*** In teleworking, the manager or employer has to check the contributions provided by the teleworkers, in a similar way that someone has to check contributions in a crowd-sensing or mass collaboration project. Management by results is the main method used to assess the performance of teleworkers. However, many managers choose to supervise teleworkers more closely, by arranging

[34] Currently available tools include Trello (https://trello.com), Asana (https://asana.com) and Podio (https://podio.com).

periodic or ad-hoc communication sessions, physical meetings, or even installing performance-tracking software. A carefull balance between teleworker freedom and supervision is required, in order for teleworking to be fruitful for both sides.

In Table 5 we present a mapping of challenges to the relevant stakeholders.

Table 5: Telework challenges identified for relevant stakeholders

	Policy makers	Employers	Teleworkers	IT experts	Sociologists, economists and researchers
Infrastructure		X	X	X	
Security				X	
Scalability				X	X
Seamless teleworking from different devices		X	X	X	X
Efficient collaboration environment and tools		X	X	X	X
Regulations/legislation	X				X
Supervision and performance evaluation, without infringing on privacy	X	X	X		X

4.4.4 Policy background, current initiatives and future policies in telework

The report by Welz and Wolf (2010)[35] provides useful information about the status and initiatives regarding telework in Europe. The main regulatory framework for telework consists of the European Framework Agreement on telework, which was signed by the peak social partners in July 2002. Prior to this agreement, regulations about telework existed in some countries (Germany, Austria, Sweden, Norway), which were introduced at the late 90's and 00's. Although the agreement is not incorporated into a directive, it creates a contractual obligation for the affiliated organisations of the signatory parties to implement at each appropriate level of the national system of industrial relations. Several countries have chosen to transpose this agreement into national legislation (Czech Republic, Hungary, Poland, Portugal, Slovakia and Slovenia). The majority of European countries, however have implemented the principles of the Framework Agreement through bipartite collective agreements. In Belgium, France and Luxembourg the agreements cover all sectors and companies; in Austria,

[35] Welz, C., Wolf, F., 2010. Telework in the European Union. European Foundation for the Improvement of Living and Working Conditions, Dublin. Available at: http://www.eurofound.europa.eu/observatories/eurwork/comparative-information/telework-in-the-european-union

Denmark, Germany, Greece, Italy and Spain the agreements have a more limited scope and do not extend to the entire workforce.

The cornerstone of the European Framework Agreement is that teleworkers have the same collective rights as their colleagues at the employer's premises and the same protection, privileges and obligations. However, discrimination may occur, and several countries have additional legislation in matters such as the assumption of costs by the teleworker, the calculation of working hours, access to training, health and safe working conditions at the teleworker's place, taxation issues, as well as privacy and personal data protection.

In the US, the latest piece of legislation is the Telework Enhancement Act of 2012, which provided a framework for U.S. agencies to offer teleworking as a viable option to employees. By increasing the number of employees who telework, the Telework Enhancement Act has three main objectives. (1) Improve continuity of operations, (2) Promote management Effectiveness and (3) Enhance work-life balance.[36]

From a regulatory point of view, of particular interest is the implementation of telework in departments of the European Commission itself. A recent Commission Decision[37] instituted telework inside the Commission Departments, covering issues such as the time schedules, training and career development, health and safety, equipment and technical support, as well as monitoring and evaluation.

It is also worth noting that in 1992, the EC created the European Community Telework/Telematics Forum (ECTF), an independent, non-profit association that provides a framework for concertation on telework and related telematics applications for Member States, by promoting the exchange and dissemination of information between telework projects and organizations interested in telework.Furthermore, the concept of telework is reflected in the principles of more and better jobs and better working conditions implemented by European Employment Strategy, Europe 2020 strategy and Guidelines for national employment policies.[38]

From a R&I perspective, the EC has launched several actions for the stimulation of telework throughout the European Union in 1993.[39,40] The principal objectives were to encourage companies to experiment with and implement telework networks, examine the practical problems associated with teleworking, evaluate technology requirements, analyse the business impact and provide support and coordination for regional and national initiatives in this field.

These trials and demonstrations were accompanied by a comprehensive analysis of the legal and regulatory constraints to telework across international borders within the European Economic Area,

---

[36] https://en.wikipedia.org/wiki/Telecommuting#U.S._Federal_government
[37] COMMISSION DECISION of 17.12.2015 on the implementation of telework in Commission Departments, http://ec.europa.eu/civil_service/docs/equal_opp/teleworking_decision_en.pdf
[38] ERM REPORT 2008 More and better jobs: Patterns of employment expansion in Europe. Available at: http://www.eurofound.europa.eu/publications/annual-report/2008/labour-market-business/erm-report-2008-more-and-better-jobs-patterns-of-employment-expansion-in-europe
[39] http://cordis.europa.eu/news/rcn/2023_en.html
[40] http://cordis.europa.eu/news/rcn/3636_en.html

and by assessments of the potential macro-economic impacts, trade impacts and change in employment patterns. They aimed at contributing to the harmonization of approaches and to a better understanding of business re-engineering.

The funding of other projects on teleworking aspects has been sparse since then. Recent project examined the sustainability of telework (SusTel, 2001-2004),[41] and the impact of teleworking on the environment and labour market outcomes (TELE, 2015-2017).[42]

4.4.5 Opportunities for policy interventions in telework

Notable opportunities for policy interventions in the eHealth area are:

- **R&I actions on telework:** We remark that many of the challenges, including regulatory and technical issues identified in Section 4.4.3 have not been thoroughly investigated, and more funding should be provided for R&I actions. More importantly, it would be necessary to capitalize on the more than 20 years of telework practice in the EU so far, identify the progress so far and systematically explore benefits and weaknesses.
- **Telework legislation:** Besides the Framework Agreement, a thorough Regulation or Directive that addresses all apsects of telework does not exist. Such a regulation should also cover employee compensation and working hours, training, health and safety, taxation, privacy and personal data protection, and more generally issues that are treated differently in different Member States and hamper the ability of teleworkers to provide services across national borders.
- **Leveling the inequalities in adoption of telework:** Although there is a global trend to increase instances of telework, there are discrepancies in the degree of adoption of teleworking practices, especially the ones referring to part-time teleworking. For example, in 2005, according to the Eurofound report,[43] in Denmark 14.4% of employees were doing telework for a quarter of the time or more, while in Italy the corresponding percentage was only 2.3%. In addition, there are inequalities remarked in Section 4.4.1 accross sectors and genders. Especially increasing the percentage of women using telework would help improve family conditions, since women usually have a higher burden in raising children. Therefore the policy of the EU and individual national governments should aim at providing incentive for companies and organisations in these countries to adopt telework practices and to level inequalities accross sectors and genders.
- **Reliable telework statistics:** There is still a lack of reliable telework statistics, partly because of the difficulty to compare different teleworking arrangements, as explained in Section 4.4.1. However, the major problem seems to be that a systematic listing of such practices, has just not been undertaken by European organisations, in cooperation with national governments. A systematic survey should not only cover employement percentages accross sectors and genders, but also the

[41] http://momsatwork.it/wp-content/uploads/2010/03/Studi_ricerche_5.pdf
[42] http://cordis.europa.eu/project/rcn/194823_en.html
[43] Eirofound, Telework in the European Union, 2010. Available on line: http://www.eurofound.europa.eu/observatories/eurwork/comparative-information/telework-in-the-european-union

technological means used for telework and the types of fixed and mobile communication access technologies.

4.5 Workplace robotics

4.5.1 Topic description

Worplace robotics refers to the conduction of labour, or the facilitation of human labour by robots. While initially used in repetitive tasks in industrial environments, robots are rapidly appearing into human social environments and are becoming involved in increasingly more complex and less structured tasks and activities.

There is a wide range of applications, from automated control systems such as self-driving cars, help and resue operations, theurapetic robots (such as robots to help treat children with autism spectrum disorders and developmental disabilities), "care" robots intended to provide physical assistance to people with disabilities in daily living tasks, robots functioning as sales agents or conflict resolution intermediaries, robots used by police forces, or autonomous weapon systems and drones (Riek & Howard, 2014).

In general, we refer to robots as embodied systems capable of directly enacting physical change in the world. We are not referring generally to intelligent agents or systems capable of interacting with humans, but on devices capable of sensing and acting on the environment. The robot itself may merely be the visible component of a network that integrates environmental sensor systems, central planning servers, cloud-based knowledge resources, and human users and supervisors (Glas et al., 2013). In addition, we consider active sensor networks or actuator networks, where a number of devices are able to sense and act on the environment.

Human-robot interaction (HRI) depends on the degree of autonomy of the robots and the type of control that a human wants to exercise. A human may need to query the human-robot network for some information about the environment, the status of work, or about the state of the robots themselves. In this case, the human does not exercise any control, but only acts as a recipient of information from a number of robots. In another extreme, a human may act as a peer node; in this case the human does similar tasks as a robot (e.g., providing some information about the environment to the robot nodes), or as a controller. Different types of control are possible (Makarenko, Kaupp, Grocholsky, & Durrant-Whyte, 2003):

- Direct control where an action or sequence of actions is sent to a number of robots, instructing them exactly for what they should do.
- Supervisory control, where the human acts as a supervisor and can periodically send commands to switch the mode of operation of robots, or to change a utility function, thus implicitly affecting their behavior.

In terms of the different layers and dimensions of HMNs as defined in D2.2, we have:

Human agency: Depending on the degree of autonomy of the robots and the type of control that a human exercises, human agency will vary. Usually, even if controlled by humans, robot actions are usually predetermined, and humans do not have the liberty to use them for different purposes or for a diverse range of activities. This is gradually changing with multi-purpose robots or learning robots. Recently, multi-purpose robots have started to appear that can carry out a variety of activities, for example different tasks at home[44] or more diverse activities, from treating patients to farming in space.[45] In this case, humans have a greater role in training the robot, either explicitly by maneuvering the robot into desired positions, or implicitly, in which case a robot employs self-learning mechanisms, like reinforcement learning to gradually learn how to behave (Andrew Bagnell, 2014).

Machine agency: In a robotic HMN, robots are the main agents carrying out activities, and they can interact with humans in their social environment. Thus, machine agency is necessarily high. As discussed above, as future robotics technology evolves so does the range of activities that robots are able to carry out, and robots will become more autonomous. Therefore, predictability of robot behavior will decrease, leading to even higher machine agency. As a last point, humanoid robots that resemble humans in appearance and movement have appeared, although used mostly for research purposes.[46]

Regarding tie strength, what interests the most is **H2M (Human-to-Machine) interaction strength**. In D2.2, the dimensions of trust, reliance and dependency were employed to characterize this strength. Humans have grown accustomed to robots that do simpler tasks or repetitive work in factories. As robots have proved to be reliable and can carry out such work efficiently, humans not only trust them, but also rely on them and have become depended on them. For example, it is now unthinkable that a car factory for mass car production can function without robots. However, things become more complicated when robots are highly or completely autonomous and perform vital tasks such as driving a car, performing surgery, and apply lethal force in police duties or in warfare. In such situations, the degree of trust will depend on the level of mistakes that robots make and the criticality of a task. In life and death matters, only an infinitesimal amount of mistakes should be allowed. However, the decision to use a robot in critical tasks may also depend on other network effects: for instance, in warfare, even if a robot is less efficient than a human, it may be preferable to risk destroying the robot than human lives. In such case, trust and reliance may occur as a necessity or as the least painful alternative.

The **network size** and **geographical expansion** of a robotic HMN are usually small, as robots usually interact with a small number of people in a limited area. An exception is the case of small robotic devices in actuator networks, where a large number of devices may be used to sense and act on the environment in a large area. However, again the actuator network will be limited to a geographical region that is not expected to exceed that of a city.

---

[44] http://www.betaboston.com/news/2014/07/16/robot-startup-jibo-unveils-a-multi-purpose-social-bot-for-the-home/

[45] http://www.cityam.com/1406213701/manufacturing-space-farming-meet-baxter-multi-purpose-robot

[46] http://spectrum.ieee.org/robotics/humanoids

Regarding other dimensions, workflow interdependence is usually small and there need not be collaboration or coordination between people in a robotic HMN. A much more advanced robotics technology would be required to enable the creation of more connected networks involving many robots and humans, which is not likely in the near future. Thus, usually a robotic HMN will have a hierarchical centralized structure with a human controlling one or more robots.

4.5.2 Stakeholders involved in workplace robotics

Stakeholders involved in workplace robotics are:

- **Policy makers and regulators**, who are interested in regulatory challenges posed by advancements in robotics and whether or not existing regulation is sufficient to address societal needs. For example, in personal data processed by robots, it may be sufficient to extend the application of the General Data Protection Regulation to the robot controller. However, this may be difficult to apply in practice, as robots may collect a tremendous amount of data, and these data may be collected for no specific purpose (i.e. as part of casual interactions between robots and humans). In general, policy makers have to strike a balance between societal needs and the promotion of technological progress and innovation, which is hard to achieve.
- **Professionals**, who interact with robots as part of their professional activity, either as controllers of robots, or for collaborating with robots (e.g. a doctor using a robot to assist surgery (see Section 4.2)). Professionals can convey useful experience about HRI, and can provide a more systematic analysis of problems and workarounds. In additional, we include professionals working in fields that are likely to be impacted by robots, such as insurance companies who are likely to insure for damage caused by robots, logistics companies who may use robots for freight transport, or marketers working in robotic products.
- **Non-professional users**, who interact with robots in normal activities. Examples are patients who use therapeutic robots, elderly people or people with disabilities who use care-robots, or even consumers who may encounter a robot-helper at a shopping mall. Such users can convey useful design requirements, may have difficulties to trust and collaborate with robots, and need more information about robot design and operability.
- **Robotics manufacturers**, who apply technological innovations to manufacture and improve robots, but may be unaware of legal or ethical constraints. Receiving user feedback is essential for them, especially for embedding practices in the initial design of a system.
- **IT experts**, who apply information and communication technologies and are involved in how a robot collects, processes and disseminates sensor data. This group of stakeholders has the important role of applying data protection rules and of dealing with practical problems that may appear for the application of such rules.
- **Researchers.** Studying HRI is an interdisciplinary field involving electrical and mechanical engineering, computer science (human-computer interaction, artificial intelligence, robotics, natural language understanding and processing, computer vision), social sciences (psychology, cognitive science, communications, anthropology), and humanities (ethics and philosophy).

Researchers from all these areas can contribute to the advancement of robotics and address societal needs.

Throughout the project, we plan to engage the aforementioned broad range stakeholders.

4.5.3 Specific challenges and high-level objectives of HMNs used in workplace robotics

We distinguish between technical and non-technical challenges. One of the technical challenges is the scalability of the system; human involvement must be designed for scalability, so that the human-robot interaction part does not become a bottleneck, for example when a human controls a very large number of robots. Scalability implies a decentralized design, where all tasks are performed in a distributed manner and the human acts as a peer of the network. At the same time, the human needs to have a global view of the system and to be able to influence the robot behavior. For controlling a large network of robots a large number of humans may also be required, depending on the degree of autonomy of the robots.

There also needs to be an adaptive task allocation algorithm, which considers the control tasks that need to be done and their priority, and then decides for the sequence of control commands sent to the robots.

In order to integrate robots successfully to the human social environment, robots must be designed to effectively recognize people and their behavior, recognize and coordinate with other robots (coordination of offered services and navigation paths), store knowledge information necessary to provide assistance to people (e.g. knowledge for giving directions to people), as well as to conduct appropriate dialogues with people and provide personalized services.

Security risks are also predominant, primarily to avoid takeover of robot control by other parties. While in a normal computer system security breaches usually affect a limited part of the system and partial operation may be possible, in a robotic system takeover of control constitutes a danger to the whole system.

Non-technical challenges are primarily related to ethical matters. Various ethical issues arise in HRI research, development, and marketing. Robots are carrying out increasingly complex and less structured tasks, and are becoming more autonomous. While this is one of the goals of robot design, it poses problems related to the handoff of control from the robot to the human controller, or about the probability of robots to ignore human will. Considerations range from design decisions about the kinds of situations in which robot-human handoff will be suggested or mandated, to designing for ease of handoff without significant interruption of control functionality, and designing for avoidance of unwarranted human operator habituation to automatic controls, such as controls that require occasional human inputs as well as preplanned episodes of handoff to the human controller for the purpose of maintaining human control skill levels (William Form, 1987).

In robots used by police or the armed forces, ethical issues emerge from the inability of robots to judge whether lethal force is necessary in a particular situation. While robots were initially used by police and the armed forces only to detect and defuse bombs, they are being used with lethal intention against humans recently. Drones are now commonly used in warfare, and recently the US admitted to drone strikes in Pakistan, Yemen and other places killing up to 116 civilians.[47]The use of a bomb-carrying robot to kill an armed suspect in the fatal shootings of five officers in Dallas sparked a debate about the righteousness of such an act, and what may happen next.[48]

In robots used for therapy, patients can often develop strong psychological and emotionally important bonds with the robot, which can negate any therapeutic benefit if treatment is stopped. Similar effects can occur by the use of robots to assist the elderly or handicapped persons, or by their involvement in particularly intimate human activities such as bathing and sanitation.

When robots engage in dialogues with humans, risks can emerge by recording the conversation, processing it to retrieve personal information, or using the recorded information for commercial purposes.

In order to safeguard human values of peace, justice and fairness, solidarity, freedom, honesty and trustworthiness, several researchers advocate for the development of a code of ethics for use in designing robotics systems. For example, Riek and Howard propose that such a code should integrate the following elements:

- Maximal, reasonable transparency in the programming of robotic systems.

- Predictability in robotic behavior, trustworthy system design, and ability to reconstruct a robot's decision path for the purposes of litigation and dispute resolution.

- Real-time status indicators and opt-out mechanisms (kill switches).

- Facilitation of human informed consent.

To these design principles, we may add transparency about the use of personal human data by robots, accountability for robot behavior, as well as design of decision support mechanisms taking into account both rationality and human values.

Finally, social problems may incur from the increasing use of robots, like the increase of unemployment by robots taking over human jobs. This has been an overarching issue from the very start of the appearance of robots in the industrial era, but it has re-emerged due to improved robot capabilities, which threaten to take over more demanding jobs such as taxi and truck driving, tourist guiding, salesmen, etc. Increased unemployment is a major social and economic problem; therefore, a smooth transition is required for the use of robots in tasks formerly done by humans, taking into account all factors.

In Table 6 we present a mapping of challenges to the relevant stakeholders.

[47] http://bigstory.ap.org/2ba0067d56e242b796b1f6eefc09f8aa/
[48] http://bigstory.ap.org/article/adff4cd6a2be49879efd661942b74311/killer-robot-used-dallas-police-appears-be-first

Table 6: Challenges for workplace robotics as they relate to specific stakeholders

	Policy makers	Professionals	Non-professional users	Robotics manufacturers	IT experts	Researchers
Scalability				X	X	X
Efficient robot design				X	X	X
Ethics	X	X	X			X
Privacy	X	X	X			X
Social problems (e.g., unemployment)	X	X	X		X	X
Regulations /legislation	X					X

4.5.4 Policy background, current initiatives and future policies in workplace robotics

The EC acknowledges robotics as a fast developing market, with diverse applications in manufacturing, search and rescue and retrieval, inspection and monitoring, surgery and healthcare, homes and cars, transport and logistics, agriculture, and many more.[49] They have funded and continue to fund a large number of robotics projects; at completion of, FP7 directly funded some 130 robotics based R&D&I projects involving around 500 organisations with total grants of some €536 million.[50] Through Horizon 2020, they fund more 100 research projects, ranging from autonomy, manipulation and grasping, mobility and navigation in all terrains, to human-robot interaction and cooperative robots.[51] In order to connect research to the market needs, a public-private partnership called SPARC has been set-up in the frame of the Horizon 2020 programme.[50] This includes pilot installations for long-term deployment of robotics systems into real environments, as well as tools to support the involvement of SMEs in developing robotics technologies.

Relevant technical directives for the operation of robots are the Machinery Directives (8/37/EC and 2006/42/EC) and the Directive for Noise Emissions for Outdoor Equipment (2000/14/EC). The Machinery Directive 2006/42/EC provides the regulatory basis for the harmonisation of the essential health and safety requirements for machinery at European Union level. It includes a safety standard for industrial robots.The Noise Directive 2000/14/EC defines noise limits, equipment, methods of measurement etc for use of machinery, including robots, in outdoor environments. Other regulatory

[49] https://ec.europa.eu/digital-single-market/en/robotics#Article
[50] http://sparc-robotics.eu/implementation/
[51] https://ec.europa.eu/digital-single-market/en/programme-and-projects/project-factsheets-robotics

instruments are Directive 2001/95/EC on general product safety and Directive 89/391/EEC on the introduction of measures to encourage improvements in the safety and health of workers at work.

On the ethical side, there are only a few ethical regulations that deal explicitly with robots. At the European level the ‘‘Charter of Fundamental Rights of the European Union’’ (2000) is the appropriate frame. In specific fields, such as medicine, the armed forces, and entertainment there exist more specific regulations and codes of practice. For example,[52]

- In medicine, Directives 93/42/EEC and 90/385/EEC concerning medical devices and implantable medical devices, respectively.
- In the armed forces, the ‘‘Common Military List of the European Union’’ (2007/197/CFSP), which serves for export control in the context of the European Union Code of Conduct on Arms Exports (1988).
- In entrertainment, Recommendation 2006/952/EC Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity.

4.5.5 Opportunities for policy interventions in workplace robotics

There is a clear need for explicit consideration of ethics in HRI research, development, and marketing. The need for a code of ethics for HRI practitioners becomes ever more compelling, as does its endorsement by relevant professional associations, this a way of encouraging at least a minimum of attention to ethical issues.

The guiding principle should be respect for human autonomy, respect for human bodily and mental integrity, and the affordance of all rights and protections ordinarily assumed in human-human interactions. Ethical perspectives should be incorporated in every phase of HRI research, development and marketing, while robotics research and innovation should be oriented towards societal needs.

The current regulatory framework also does not sufficiently take into account the legal implications of robotics.[53] Among the topics where guidance is required are liability rules and insurance for protecting against damage caused by robots, protection of data that is retrived and disseminated by robots, cyber security and regulation of human enhancement (i.e. the use of robots to enhance human capabilities).

Addressing which kinds of labour can be done by robots and which cannot is a task that also has not been investigated. This is an issue that not only concerns the appropriatness to use robots, their technical competence and efficiency, but also the effects on employment and loss of jobs, as well as ethical considerations (what kinds of labour are considered as humane or inhumane).

In addition, policies that support equal access to robotics must be devised and implemented, including sustainable business models, so that everyone can enjoy the benefits of robot technology to assist human life.

---

[52] Nagenborg, Michael, et al. "Ethical regulations on robotics in Europe." Ai & Society 22.3 (2008): 349-366.
[53] https://www.theparliamentmagazine.eu/articles/opinion/eu-robotics-rules-right-time-address-ethical-issues

4.6 Decision support systems for crowd management

A decision support system (DSS) may be defined as "[a] computer system specifically designed to assist users in making unstructured or semi structured decisions, i.e. the nature of the problem requiring a decision is known in advance" (Law & Smullen, 2014), and as such would cover any automated system taking in data in various forms and on the basis of a given algorithm generates one or more possible matching outcomes. The "users" would then typically be able to respond either accepting the automatically generated outcome or choosing a different solution, usually integrating their own experience as a moderator to that outcome. Typical DSSs would theoretically include anything from recommender systems for online retailers based on past purchase or browsing history, as well as credit checking for a loan or hire purchase agreement, and even a selection of suitable holiday destinations based on the selection of dates, number of people travelling together, and location. Although retailers like *Amazon* encourage the exchange of feedback as well as sharing experience and responses to specific questions, these DSSs are little more than machine algorithms and do not qualify as full HMNs. For DSS networks involved in crowd management, therefore, we expect increased complexity. But in addition, there would typically be two network operational states: first, a *monitoring* state when the crowd is being observed via sensor input by the DSS and operational staff; leading to a second more proactive *management* state, should an incident occur and the crowd need to be assisted, potentially involving intervention from emergency services such as paramedics, the police, the fire service and even special forces.

4.6.1 Topic description

Over recent years and not least in response to highly publicised disasters such as the 2004 Indonesian tsunami (Strunz et al., 2011), (Leone, F. Lavigne, R. Paris, J-C. Denain, 2011) or the 2011 Fukushima incident (Noggerath, Geller, & Gusiakov, 2011), (Lipscy, Kushida, & Incerti, 2013), there has been a growing trend to extend simple monitoring systems which are prone to being ignored or overridden (Norman, 2011) to provide full HMN-capable decision support capabilities whereby human operators and participants interact collaboratively with machine components towards the safety and security of the crowd in question. Projects such as TRIDEC (http://www.tridec-online.eu/) and ANYWHERE (http://www.anywhere-h2020.eu/en/about-anywhere) focus on extreme weather and similar crises, whilst eVACUATE (http://www.evacuate.eu/) is geared towards the safe evacuation of crowds from confined areas such as stadia, ships, and public transport hubs. In all of these cases, three groups of human actors tend to group around the DSS: members of the public / evacuees who are being monitored and supported to safety; operational staff responsible for the smooth and continued operation of information gathering and response co-ordination; and emergency services who may be called in to assist. The machine actors within the network typically include the DSS itself along with the distributed remote sensors providing the main source of incoming data, and any access devices or interfaces the human actors used to interact with the DSS.

Decision support systems for crowd management therefore represent complex HMNs where human actors must respond to the machine actors to reach a common beneficial outcome. However, there are specific issues that tends to set them apart from other DSSs as well as other HMNs.

4.6.1.1 Practical issues: network dynamism

Unlike many other HMNs, DSS must cater for two types of dynamic change in human and machine actors. First, those being monitored will typically be no more than passive data or information sources under standard operation. Only in the case of some kind of emergency or crisis do they become a significant part of the overall decision making and operational effectiveness of the network. At the same time, operational staff responsible to those members of the public may well be joined if needed by emergency services who then share responsibility and may even assume overall control. Secondly, and referring specifically to machine actors, this may lead to a requirement to be able to connect and integrate multiple other machine components and devices as required by any particular subgroup, such as emergency service personnel, or becomes available, such as smartphones.

HMNs for decision support in connection with crowd management must therefore cater for changes in the number of nodes and the complexity of the interactions between them.

4.6.1.2 Operational issues: information overload

A significant motivation behind many decision support systems was originally to capitalise on data mining techniques to be able to handle large amounts of data.[54] One or more operator would be overwhelmed and was certainly not adept at correlating and integrating data from multiple sources. Human actors therefore lack the ability to process the volume of information essential for developing an overall picture of a situation and therefore to be able to arrive at a suitably grounded decision. What human actors bring to bear, though, is experience and sensitivity to a situation especially when faced with difficult moral dilemmas such as when to withdraw emergency services or when to divert resources to more appropriate targets. There is a synergy and interdependence between human and machine actors that emphasises the uniqueness of decision support systems.

HMNs for decision support in connection with crowd management still need to be able to integrate empathy and experience from human actors with the objective results from data processing.

4.6.1.3 Ethical issues: technology making life and death decisions

There are certainly obvious data privacy issues surrounding decision support. Using data from monitoring crowds could be misused,[55] and potentially lead to the identification of wrongdoers. Although illegal when such profiling is carried out automatically, data protection is less important as the vital interests of the human actors. What is important, though, is when automatically generated 'decisions' are incorrect: machine algorithms may contact errors ("bugs"), a data source missed, or incorrect assumptions made. This is not simply a question of rogue computers like HAL in *2001: a Space Odyssey*, or using noughts and crosses to avoid nuclear war in *War Games*. This is a question of transparency and making informed decisions. Because of this, it is clear that however significant the

[54] See, for instance (Gianpaolo Cugola, 2012)

[55] Cf. using social media posts after the 2011 London riots to convict those involved (https://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf)

role of the machine actors in providing computational support, the ultimate responsibility should always lie with one or more human actor.

Final responsibility within HMNs for decision support must always reside with human actors. There may even be a case for making human override possible at all times.

4.6.1.4 Societal issues: prejudice/ingroup/outgroup

Above, we have alluded to instances where human intervention should be supported if not required as an appropriate counter-balance to machine objectivity and a failure to mediate any algorithmically derived decisions. However, there is a significant feature specifically in respect of the human actors in the network which needs to be considered. Consider the main categories of human actors: first there is the operational staff responsible for managing whatever situations arise and interacting most regularly with the machine nodes; second there are the emergency services which may or may not be brought in to deal with a more serious development; and finally, there are the individuals being monitored to begin with but subsequently to be informed and managed for their own safety and security. The dynamics of the relationship between the different groups, but also within the same category. Operational staff may resent having to relinquish overall command to the emergency services; this is not surprising. More significantly, however, the emergency services may provoke uncooperative even hostile responses in those they are seeking to help (Drury & Reicher, 2000). Similarly, any separate groups within the citizens to be helped may not willingly cooperate[56],[57] (Tajfel & Turner, 1979), Taylor, 1990; (Scraton, 1999); (Challenger, Clegg, & Robinson, 2009), but must be encouraged to establish dynamically new and effective groupings (Levine, Prosser, Evans, & Reicher, 2005) in response to a current crisis and draw on natural tendencies for mutual support (Franco & Zimbardo, 2006).

Beyond the role of machine actors in DSS-based HMNs, interactions between human nodes must be channelled towards mutual support and cooperation to avoid destructive social categorisation.

Returning for now to the analytical layers proposed in D2.1, the following should be noted in respect of Decision support HMNs for crowd management:

Agency: both human and machine agency vary over the typical lifecycle of a decision-support based HMN. On the one hand, the numbers and categories of actors will vary as the DSS moves from simple monitoring to a more active engagement with crowd management in a crisis or other unusual event. For example, during regular monitoring, only operational staff would be actively engaged in checking status. The DSS itself would be processing information at an almost constant rate, with sensors or

[56] The Hillsborough Stadium Disaster. Inquiry by the Lord Justice Taylor (1989). Available on line: http://www.southyorks.police.uk/sites/default/files/hillsborough%20stadium%20disaster%20final%20report.pdf

[57] Understanding Crowd Behaviours: Supporting Evidence. The Cabinet Office Emergency Planning Office, York, UK (2009). Available on line: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192606/understanding_crowd_behaviour-supporting-evidence.pdf

peripheral distributed devices acting as passive receivers of data. Agency is therefore moderate and confined to specific nodes.

Should some form of incident occur, this will change. Machine agency immediately increases, with at least CPU load and throughput increasing as more, possibly targeted information is processed. Further, peripheral devices will typically change in one of two ways: first, input from specific devices will be orchestrated to focus on specific types of information, the devices themselves may even be configured for greater accuracy etc.; in addition, communication with the devices may become half- or full-duplex as commands and content are sent to the devices (such as signage). At the same time, human agency increases as operational staff engage more directly with the DSS and appropriate procedures for a given incident. Further, other categories of human actors – emergency staff, but especially the crowd to be managed – will engage and begin to interact as well.

Interactions: once again, the frequency and nature of interactions between the various actors change depend on the state of the HMN: for regular monitoring, the main interactions occur between operational staff and the DSS itself; emergency services are not involved at this stage at all; and those being monitored may be unaware that they are being observed at all, acting as passive nodes with the network.

As soon as the DSS network begins to respond to an identified issue, then existing interactions are intensified: specifically, operational staff now begin to interrogate the DSS and may even direct what information is gathered and aggregated. Beyond that, though, H2H interactions intensify as dependence, reliance and trust comes into play. Further, category internal interactions may well have an effect: if different groupings within the crowd to be managed do not begin to cooperate with one another, the crowd management objectives will become more difficult to achieve. Further, inter category interactions (police to crowd, for example) may exert a detrimental influence over the overall efficacy of the network.

Behaviours: when the network is being used primarily to monitor a given situation, the network is largely top-down for the operational staff and the DSS itself given that the system functions along fairly rigid and pre-defined lines; similarly, workflow interdependence tends to be fairly high, with the DSS and operational staff working in sync and one step for either directly dependent on a previous step. At the same time, the crowd being monitored are anything but fixed and predictable beyond the specific confines either of the physical location or behavioural context (a sporting event, a show, a cruise, etc.): network organisation is dynamic and largely bottom-up; and inasmuch as there is any 'workflow' it is very low – what one person does is largely independent of what other people do.

This all changes, of course. One of the main challenges in crowd management is to encourage interdependent and complementary working, in a largely top-down environment. The goal is to effect safe management of the crowd irrespective of the particular situation and that will inevitably involve conformity to a limited set of plans or procedures. In respect of behaviours, therefore, DSS HMNs are all about looking for activities which fall beyond the expected or desired at some level, and which therefore tend to reflect a bottom-up evolution of the network and a less coherent set of interactions.

Network: the geographic extent of a DSS HMN remains relatively constant, since of course a crowd management system will be focused on a specific area. This is not to say that information from other sources further away may not be used at any given time. For instance, civil disturbances in different parts of a city may need to be co-ordinated by the authorities to avoid escalation (see (Waddington, 2012)).

By contrast, the size of the network can and does change considerably over time, and not only in response to a shift from crowd *monitoring* to crowd *management*. Both machine and human nodes are likely to change in response to monitoring in different sub areas, but also as the number of people observed changes, for instance, as a train arrives in a station. The most dramatic changes do occur during the management of any specific incident: machine nodes may increase if emergency services are involved, and if different peripheral devices are recruited or reconfigured to help provide additional or more specific information. At the same time, roles and responsibilities may change across the human nodes, not least as crowd members become active participants in how they are managed.

4.6.2 Stakeholders involved in decision support systems for crowd management

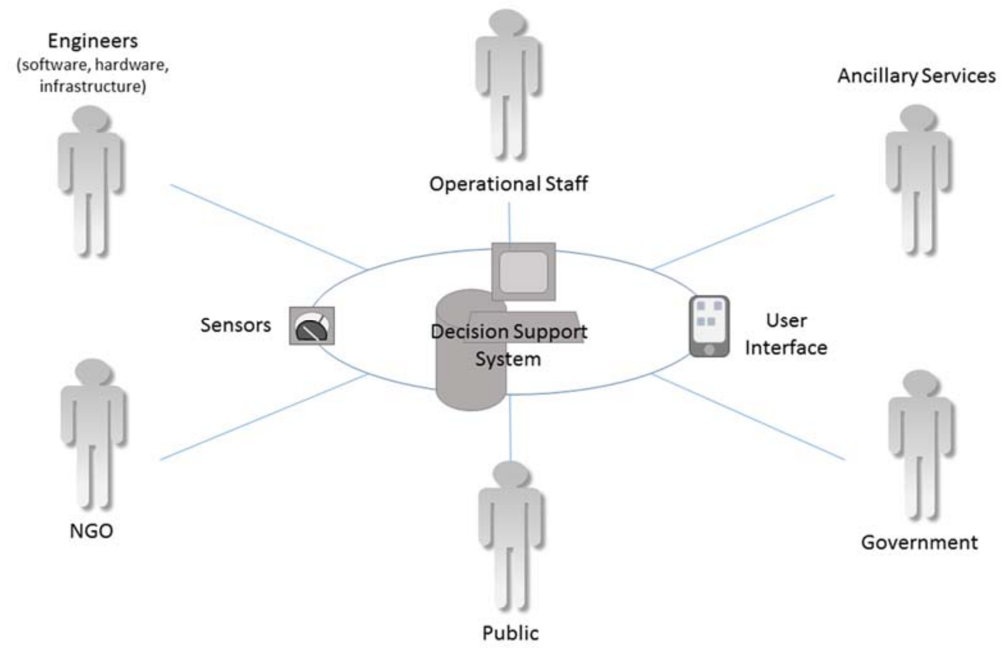

Figure 4: Main stakeholders interested in how decision support systems (DSS) operate and evolve

The main stakeholders involved fall into two categories: those directly involved in the network (*participants*) and those with simply an interest in the network (*interested parties*). This distinction affects their respective attitudes, as well as what they might contribute to the roadmap.

The stakeholders may be described as follows:

- **Engineers** *(interested parties)***:** those building and maintaining the infrastructure, that is the machine elements within the network; they may or may not be responsible for the entire infrastructure since sensors could be provided separately and as part of a city- or network-wide resource for instance;

- **Operational staff** *(participants)***:** those responsible for the day-to-day exploitation of the decision support system based on the network;
- **Ancillary services** *(participants)***:** any of the emergency services (ambulance, police, fire service, terrorist units, etc.) who will become involved *ad hoc*;
- **Government** *(interested parties)***:** who carry the ultimate responsibility for the safety and security of its citizens;
- **The Public** (*interested parties* and *participants*): members of the public are interested in the level of surveillance irrespective of purpose and location; this is an issue of civil liberty. However, at the same time, they may well be *involved* directly in some incident or at some place where active or passive crowd management is in place;
- **Non-governmental organisations (NGO)** *(interested parties)***:** again, from a civil liberties' perspective, NGOs are primarily concerned with the ethical use of any monitoring equipment, but also in the efficacy and benefit of any automated DSS.

Across these stakeholders, a number of themes should be explored in relation to the use of decision support systems for crowd management. The engineers are more concerned with the development and delivery of the solution, and as has become apparent through some of the case engagement reported in WP2 and WP3, they have less of a focus or interest in the dynamics of human participation, but rather the robustness and reliability of the DSS platform itself. Encouraging direct engagement between engineers and other stakeholders, not simply under a general UCD umbrella but also to understand the broader ethical, legal and motivational issues associated with the HMN within the context of its appropriate ecosystem.

One of the most important aspects of engagement with Operational Staff is to understand their motivations and expectations from working together with a DSS platform, but also with any Ancillary Services which may be brought it. It is up to the Engineers to understand how they operate and what they do; this will help identify the objectives of these nodes within the network. But there are more significant issues for Operational Staff. For example, will they perceive the DSS platform as supportive in connection with their responsibilities? Where do those responsibilities end: legally[58] and spatially?[59] Extending the responsibility to include Ancillary Services, the main questions to be explored and understood include how they would wish to integrate their own activities and indeed their own HMN into the broader crowd management network. There are specific technical issues such as interfaces, privacy and governance. But there are procedural issues too about access and chain of command.

As stakeholders, Government and NGOs provide a balance for one another. Government has, as we said, a responsibility to its citizens. And surveillance provides an effective means of monitoring what's going on. Understandable nervousness arises though at the thought that surveillance for safety may

[58] Duty of care is a moral obligation under Common Law, but a legal one under Civil Code.
[59] Is safely guiding a substantial crowd out of a venue enough? Or does there need to be some management of that crowd once they are outside and in the surrounding area?

extend beyond its original intention and become a tool for control: the mismanagement of the unrest following the Mark Duggan riots illustrates the point (Waddington, 2012). Government do therefore have an important view on the objectives of DSS networks, and how they should be taken forward.

At the very boundary of what is acceptable under the European Charter of Human Rights (especially Articles 8, 10 and 11[60]), surveillance is a sensitive subject and this is where NGOs tend to engage on behalf of the Public. In providing some level of independent oversight, NGOs can provide a helpful mediation role between Government and the Public. Their views may be expected, therefore, to provide a useful background against which to attempt to evaluate the significance of views expressed both by Government and the Public.

The final group of stakeholders who should be approached in the context of DSS systems for crowd management is the Public themselves. On the one hand, passive subjects of observation, but also the main beneficiaries through direct participation as well as in the guise of an interested 3rd party, the Public may provide multiple and occasionally contradictory perspectives on how DSS HMNs should be developed and operated. For, although personal privacy may *a priori* be regarded as paramount, there may at the same time be an appreciation that personal safety requires some compromise[61]. Engagement with this group of stakeholders may therefore need to involve multiple, separate sessions to ensure that these issues in connection with DSS HMNs can be examined independently.

4.6.3 Specific challenges and high-level objectives of HMNs used in decision support systems for crowd management

In the introductory sections above, we discussed some of the major issues relating to DSSs for crowd management (see Sections 4.6.1.1 to 4.6.1.4). Here we will return to these issues and consider specifically how these should be managed in the development and deployment of such HMNs.

<u>**Technical challenges**</u>:

Given the significance of DSS systems, in terms of the potential to save lives and avoid significant and unwelcome incidents, the main technical issues include:

- **Robustness:** for the purposes of this discussion, we may define "robustness" as the capacity for a node or nodes in the HMN to cope with disruption, including power outage and the likely, and thus provide a continuous, uninterrupted service. This is a specific issue for the machine nodes, requiring appropriate engineering approaches to avoid downtime for maintenance, cater for failover and redundancy, and mirror essential information.
- **Reliability:** here, we define "reliability" in terms of how good the information aggregations and conclusions that the DSS generates turn out to be[62]. Clearly, it is essential that outputs from the

[60] http://www.echr.coe.int/Documents/Convention_ENG.pdf
[61] https://www.theguardian.com/world/2015/jan/06/tony-porter-surveillance-commissioner-risk-cctv-public-transparent
[62] There is an interesting indirect issue here related to robustness. Suppose, for instance, a communication link is lost between one or more sensors and the DSS platform itself. It may be possible, especially based on past experience, to interpolate any missing data which may result from the loss of the connection. However, the

DSS platform and across the whole HMN must be reliable. This may involve ensuring transparent algorithms being used to allow for rapid and clear checking; or multiple algorithms being used to calculate the same value. It may also involve prioritising activities to ensure that the most relevant information / outcomes are presented first.

- **Flexibility:** by definition, the HMN needs to be able to cater for a number of different situations. A heavy holdall may contain a weapon or some such on one occasion, but simply be luggage on another. More importantly, though, the HMN needs to be able to accommodate changing numbers and types of node. As previously stated, the Ancillary Services for instance would bring in new human nodes at least, but may also involve the temporary connection of additional devices.

These technical issues need to be planned for during design, development and of course deployment. Any specific problems which may occur must not be allowed to compromise the safe, effective and continuous use of the DSS network as it supports crowd management activities from simple observation to direct intervention and control.

Non-technical challenges:

There is a common misconception that crowds will panic in crisis situations. This is purported to be based on the early work by Le Bon, though in reality simply perpetuates a common misinterpretation of the work[63]. It is more realistically attributable to an observation that during the first moments of a catastrophic event, individuals may become confused and simply look to escape immediate danger often caught up by physical restrictions (Helbing, Johansson, & Al-Abideen, 2007). If this view were true, then the major non-technical challenge would rest with trying to avert panic and forcing individuals in the crowd to stay calm. Of course, all of this fails to recognise the enormous weight of empirical evidence that paints a completely different picture. Faced with extreme danger, individuals are much more likely to co-operate and provide mutual support even to their own detriment[64] (Blake, S. J., Galea, E. R., Westend, H. and Dixon, 2004); (Fahy, R. F. and Proulx, 2002).

The major non-technical issues may therefore be summarised as:

- **Ethics:** there are two specific issues here. First, as previously outlined (Section 4.6.1.3), given the significance of decisions being made, ultimate control must always lie with the human actors within the network. Secondly, there needs to be some independent governance (probably non-governmental) which would decide when the best interests of those being monitored (their "vital interests") merit observation and interaction beyond what their normal Human Rights would dictate in terms of privacy, but also consent.

---

utmost care must be exercised since there will come a point at which the interpolations cause any resulting conclusion to be worthless and compromise the DSS.

[63] Le Bon's thesis is really about deindividuation under certain specific circumstances such as political protest. Under such circumstances at the very least group processes will tend to come to the fore in relation to strong and heavily entrenched in- and outgroup boundaries.

[64] What do the events of 9/11 tells us? Drury, J. (2011) Available on line: http://drury-sussex-the-crowd.blogspot.co.uk/2011/09/what-do-events-of-9-11-tell-us.html

- **Legal:** the main legal issue (beyond privacy and data protection) relates to the automatic profiling of any individual that could lead to their arrest or act in some way to their detriment. Clearly a DSS would benefit from being able to identify potential wrongdoers or criminals in a crowd to be able to remove them for the benefit of the majority of the crowd. This may even mean claiming that the vital interests of others in the crowd are best served by doing this. However, this view is one-sided and fails to exploit lessons from social psychology research. Such 'profiling' should not only be directed towards the crowd themselves, but also towards any other groups (Operational Staff and Ancillary Services) who may be encouraging negative and aggressive behaviours albeit unwittingly by their response to the crowd (Drury & Reicher, 2000); (Waddington, 2012).
- **Agency:** it is tempting to assume that agency – the ability of any particular node or nodes to initiate activity – comes down to the issue of responsibility discussed above. However, there is a more subtle issue related to agency. To different extents, all of the components within a DSS HMN may be expected to become maximally active: machine nodes must process huge amounts of information from different sources quickly and reliably; operational staff must respond to threats and attempt to avoid them becoming full-blow problems; ancillary services must guarantee the safety and security of all involved; and members of the public must behave sensibly in response to whatever directions they receive. However, it is the interdependence of agency which is more important: all nodes, whether human or machine, must operate together and collaboratively for the network to achieve its overall goals.
- **"Panic":** as previously stated, people do not panic after the initial stages of an incident; although extreme confinement may result in unwanted consequences (as has happened on occasion at the Hajj: which is actually about the density of the crowd and physical / environmental constraints (Helbing et al., 2007); (Challenger et al., 2009). That being said, all components of the HMN must react very quickly to assume control in crisis situations to demonstrate across the network what the overall strategy will be and that help is available. In short, to facilitate co-operation as quickly as possible, all nodes must be encouraged to work in tandem towards a common objective and the overall benefit of the network. For this to be effective requires all of the other non-technical issues to be suitably managed: ethical and legal issues must not be allowed to act as a barrier to effective decision support, and high ("chaotic") human agency must be reduced to facilitate a high degree of workflow interdependence and top-down network organisation. It should not be assumed, however, that this rests solely with the machine nodes: human-to-human collaboration must be effected quickly, as well as the redrawing of ingroup / outgroup boundaries if necessary.

These challenges affect the stakeholders described in different ways. This is summarised in Table 7:

Table 7: Challenges for decision-support systems for crowd management as they relate to specific stakeholders

	Engineers	Operational Staff	Ancillary Services	Government	NGOs	Public
Robustness	X	x	x			x
Reliability	X	x	x			x

	Engineers	Operational Staff	Ancillary Services	Government	NGOs	Public
Flexibility	x		x			
Ethics		x	x	x	x	x
Legal	x[65]	x	x	x	x	x
Agency	x[66]	x	x			x
"Panic"	x	x	x	x	x	x

These specific issues may form the basis for broader discussion with different stakeholder groups, or alternatively, a common theme, such as legal issues for all stakeholders, robustness for some etc., could be used as the basis for a focus group involving stakeholders of different types.

4.6.4 Policy background, current initiatives and future policies in decision support systems for crowd management

Despite a long history of natural and man-made disasters (MORI & TAKAHASHI, 2012), there is still very little co-ordinated discussion and policy on crowd management[67]. Whilst the Hague Programme[68] stresses the need to protect justice, freedom and security for all EU citizens, derivative and associated programmes such the EU Crisis Coordination Arrangements[69] and the rapid alert system, ARGUS,[70] seem to focus on security and Member State collaboration and coordination at a macro level. As such, technology, especially for communication and connectivity, and procedures are emphasised rather than more specifically network-oriented analysis and recommendations. Policy therefore seems to be directed towards monitoring, surveillance and control.

The UK Health & Safety Executive go some way to redress the balance implicitly by identifying hazards that may be associated with the crowd themselves in contrast to those associated with the environmental context (the "venue").[71] Taxonomy of potential threats categorised in this way may provide a helpful starting point in identifying preventative measures for some specific cases. However, it fails to recognise either that some hazards may well be unavoidable ("Sources of fire, such as cooking

[65] In the GDPR (April, 2016), *privacy by design* is set to become a legal requirement
[66] The platform must be built to encourage and support agency and different levels of interaction
[67] The USA seems to be a lot more active, with local police authorities and similar groups offering advice, guidance and training (see http://lib.post.ca.gov/Publications/CrowdMgtGuidelines.pdf in California; the Oakland Police Department: http://www.nlgsf.org/sites/default/files/docs/OaklandPolicePolicy.pdf; and even the National Retail Federation https://nrf.com/sites/default/files/Documents/Crowd%20Management%20Guidelines%20Final_0.pdf)
[68] http://ec.europa.eu/home-affairs/doc_centre/docs/hague_programme_en.pdf
[69] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/crisis-management/index_en.htm
[70] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0662:FIN:EN:PDF
[71] http://www.hse.gov.uk/event-safety/crowd-management.htm

equipment") or random ("Failure of equipment") or to distinguish volition from constraint ("Crushing against fixed structures", etc.). The various sporting venue tragedies have illustrated on many occasions that official responses to such events can simply compound if not exacerbate the issue[72] (see also (Scraton, 1999); (Challenger et al., 2009); (Drury & Reicher, 2000); and periodic crushes at the Hajj[73] especially in the context of the Texas rock concert crushings[74] that crowd members may be constrained by circumstances beyond their control and which prevents mutual support and care.

Not least in response to disasters such as the Hillsborough football stadium (see above), the Civil Contingencies Secretariat funded an extensive study on crowd management by the University of Leeds (Challenger et al., 2009). As well as an exhaustive literature covering both academic research as well as official reports and eye-witness testimony, the authors reviewed a range of scenarios and identified a number of specific recommendations which go beyond a simple labelling of risks. Of these, in the present context, four of their key messages are of particular relevance:

1. *Planning should be system-wide*: it is of little use concentrating on isolated features of the (technical) infrastructure or procedures; there needs to be a **system-wide approach** involving all actors within the network;
2. *Coordination between agencies*: recognised by other government agencies (see the footnotes to this section), it is essential that **all relevant parties work together** to achieve the overall goals of the network (e.g., safe evacuation);
3. *Communication with the whole crowd*: as well as relevant parties and agencies working together and communicating with one another, it is essential to **keep the crowd informed** about what's happening and what needs to be done; and
4. *Leadership and guidance for the crowd*: group forces are very powerful; encouraging one or more individuals ('seeds'), may have a **beneficial knock-on effect** across the whole crowd.

The most important thing about these reports though is that no group or technology, no single node in the HMN, is regarded as more or less important. It is the entire network that must work collaboratively to achieve a successful outcome for that network.

[72] http://www.bbc.co.uk/sport/football/32388297
[73] http://www.theguardian.com/world/2006/jan/13/saudiarabia 1990 with over 1400 deaths due to stampede; 1994: 270 deaths; 1998: 118 deaths; 2001: 35 deaths; 2003: 14 deaths; 2004: 251 deaths; 2006: 346 deaths
[74] http://www.crowdsafe.com/cafe/who20.html

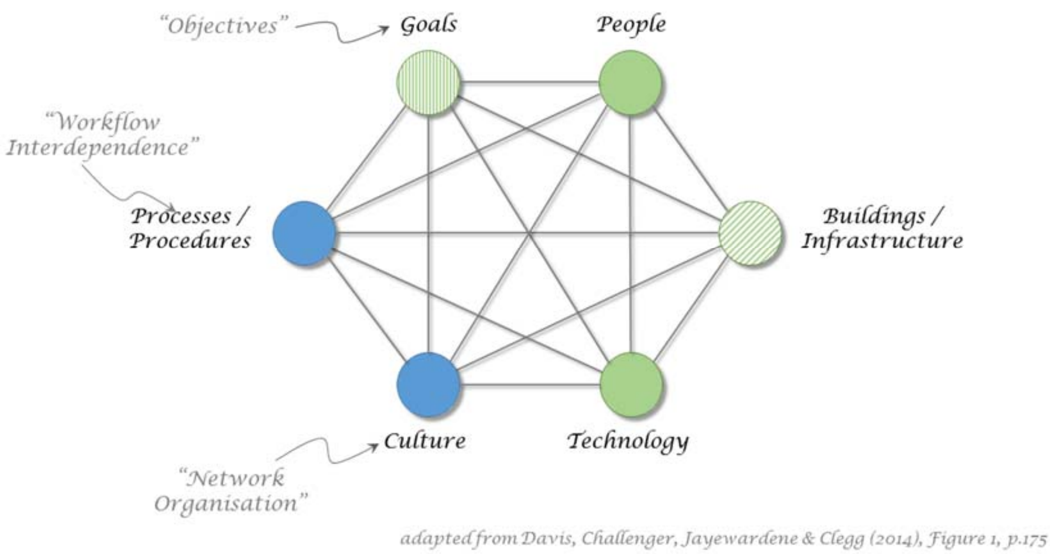

Figure 5: the complex and pervasive interactions across a socio-technical system for crowd management

Davis and his colleagues developed these ideas further in support of an integrative and fully co-ordinated socio-technical system (Davis, Challenger, Jayewardene, & Clegg, 2014); see also Figure 5 above). A complete view of an HMN as a set of collaborative interactions between human as well as machine agents is clearly significant. In this deliverable, we have further introduced the notion of the objective(s) of the network, which as shown, corresponds with Davis et al.'s "Goals". Further, and as discussed above where Human and Machine agencies affect one another subordinated to the overall objectives of the network, their "Processes / Procedures" could relate to our "Workflow Interdependence" and "Culture" to "Network organisation".

The policy and consultative background to decision-support systems for crowd management may be restricted to generic, macro-level concepts of freedom and security. But practical experience advocates instead for a meso- and micro-level coordination of resource and interaction across the *entire human-machine network*.

4.6.5 Opportunities for policy interventions in decision support systems for crowd management

In light of the previous section, some specific recommendations would be appropriate for discussion with policy makers and similar agencies. These are summarised in the following.

All nodes are equal: there is little point in focusing only on some parts of the network to identify possible issues and challenges to be overcome when the decision support system is to support crowd management. All nodes, both human and machine, are instrumental in the successful functioning of the network. However, this may also mean that human and machine nodes must be treated differently. For example, human nodes will be subject to social forces; machine nodes will not. Machine nodes will tend to be deterministic; human nodes will be less predictable. *Any policy should therefore take* *account of all nodes and node types in an HMN, reflecting the different needs and characteristics of those nodes.*

Regulatory framework: whilst protecting the rights of individuals within the network and how they operate, ethical and legal issues and challenges need to be viewed in relation to the importance of the overall objectives of the network. For instance, although privacy is an important principle, it may be sacrificed in the interests of national security. However, there must be suitable governance and checks to ensure data and information are used solely within the network and for the express purpose of its contribution and relevance to successful outcomes for the HMN. *Future regulatory policy should oversee the managed exposure of personal data in sole pursuit of the objectives of the network.*

Coordination: to facilitate appropriate collaboration across actors within and associated with the network, it is essential that all mechanisms be in place to encourage and support the coordination of activities. This would include though is not confined to a well-established but flexible chain of command to ensure that there is no time lost or wasted during operation. All agencies likely to be involved in the HMN should have clear, pre-defined relations and recognised roles within a crowd management situation. There must be no intergroup prejudice or rivalry. *Any policy on coordination should encourage open and well-managed collaborative efforts.*

Communication: in order to make sure that all nodes are kept informed of the current status and progress of any crowd management activity. This does relate to machine nodes and not just human nodes: machine nodes should receive timely indications of system status to be able to apply appropriate measures to deal with any given situation; likewise human actors will respond better if they are part of any negotiation and activity, and more likely to develop a shared sense of responsibility thus encouraging collaborative behaviours. *Policy should seek to encourage but also mandate open and frequent communication.*

Socio-technical Systems: Decision support systems should not be seen as technology 'managing' people and their activities. Especially in the context of crisis management, all nodes across the network are important and can influence the ultimate success or otherwise of the network. As such it is essential that the network should be viewed and managed as a whole. Different human actors engage at different levels and for different reasons with machine nodes. But ultimately all must work together to encourage a common understanding of any problem and to find a solution to that problem. *Any future policy for decision support systems must include all network players, and not simply machines or official agencies.*

The insights from HUMANE in terms of networks allowing for the synergistic cooperation of all actors within the network clearly has a significant part to play in informing all stakeholders about the desired future for HMNs.

5 Summary of key challenges and objectives, and their implications in HMN design

Within HUMANE, the typology and method derived from D2.2 will be applied to support future thinking on HMNs and allow for strategic discussions and policy developments of relevance to the future design of HMNs. For example, current and expected near future HMNs may be analysed with regard to their characteristics and related implications. On this basis, one may discuss how the current characteristics need to change to achieve the desired goals, and how such change may be driven through strategy and policy development.

In D2.2, we have categorized implications of HMN design as follows:

- User motivation and experience (motivation, attention, experience, reputation, information overload)
- User behaviour and collaboration (collaboration, loyalty, behaviour change, shared responsibility)
- Innovation and improvement (product quality, network growth)
- Privacy and trust (trust, privacy, security)
- Technical infrastructure (architectural, memory, and computational requirements, resilience)

In this section we summarize the most frequently encountered challenges identified in the selected social domains (sharing economy, eHealth, citizen participation, telework, workplace robotics, decision support for crowd management), and discuss the implications that these challenges have.

Technical challenges:

Data security: This is a challenge which was identified in most social domains. The security risk can be higher in more critical social domains, such as eHealth, or in domains where some applications rely more heavily on wireless technologies and autonomous systems. In such cases, there is a need for additional security practices and protocols, in extension to those used for data in general. Improving security is naturally related to privacy and trust, and enhances network resilience. Additionally, it would improve user motivation to participate in such networks.

Scalability: This challenge is also important in HMNs where data is huge such as in sharing economy and eHealth. While scalability usually involves the efficient handling of significant amounts of data, it may also involve the communication infrastructure, as in the scaling of a VPN for a very large number of teleworkers, or the control of a large number of robots. Effective scaling of HMNs also improves user experience and mitigates information overload.

Collaboration environment and tools: Collaboration is an inherent part of the sharing economy. Moreover, this challenge affects HMNs in domains such as telework and decision support for crowd management. While in teleworking, collaboration aims to the facilitation of work in the long term, in decision support for crowd management it has a more urgent nature, requiring quick decisions in a small amount of time. User friendliness, capability for synchronization of online and offline work, and logging of collaboration progress are important for the success of HMNs in such domains.

Policy challenges:

Regulations/legislation: Almost in each domain, the need for new regulations/legislation has been identified for different reasons. For example in telework, there is a lack of regulation since telework relies mainly on collaborative agreements. Also there is lack in regulation for the employment status of teleworkers, the eligibility criteria, the workplace conditions and safety of teleworkers, issues about IPR, and personal privacy. Lack of legal clarity exists for the operation and marketing of eHealth applications. Fragmentation of legislation was identified in the sharing economy, which may create confusion and endanger competitiveness.

Cost and business models: This policy challenge touches primarily on the sharing economy and eHealth. The sharing economy proposes an alternative economic model, but the synergies with existing models and the sustainability of a collaborative economy must be further studied, in order to find how to promote it more efficiently. eHealth is an example of a domain which is socially critical, but demands technological advances which are usually costly. Such HMNs require high cost for setting up the infrastructure, operation and maintenance, and without sustainable business models risk to create a technological divide between classes of people

Ethical issues: Ethical issues were primarily discovered in robotic systems and decision support systems for crowd management. In robotic systems, they involve the loss of human control due to larger autonomy and independence of robots, the use of robots by some people against others, or the creation of social problems such as unemployment. In decision support systems for crowd management, ethical issues concern the invasion of private life, manipulation of people as well as the need for careful consideration on decisions that impact on a large number of people. In both cases, there is a need to safeguard human values such as peace, justice and fairness, solidarity, freedom, honesty and trustworthiness, safety, equality, and life itself.

6 Future policy interventions and recommendations for R&I Actions

The policy landscape described in this document as well as other deliverables for the HUMANE project is clearly large and complicated. There is not a straightforward line of approach, even for clearly defined policy problems. Instead, in the areas that we have argued are particularly dependent on human-machine networks there exists a complex web of technologies, people who make the technologies, people who use the technologies, and interactions among various groups of people and technologies. All of this is operating within systems involving organizations, social and cultural norms and values, laws, regulations, economies, and the natural world. In such a complex ecosystem, what policy interventions can support responsible research and innovation of human machine networks?

In this section, we summarize the identified opportunities for policy interventions in each domain, so as to better identify similarities of approaches.

The **sharing economy** is marked by distributed networks of individuals utilizing information technologies to collaboratively produce goods, create value in otherwise underutilised assets, enable decentralized trade and consumption, and reconfigure models of ownership and value. Of course, all economies throughout history have been about sharing assets, goods and labour via trade networks and various exchange mechanisms, but contemporary sharing economy models specifically leverage human-machine networks to enable a radical combination of global networks with decentralized peer-to-peer exchanges. Thus, while one could always have let a distant friend-of-a-friend from out of town stay in their home or get a ride to the airport, AirBNB and Uber (and similar tools) let what we might think of as a “friend-of-the-network” access to similar benefits.

These sharing economy innovations operate in a number of sectors, including (as discussed earlier in this report) transportation, accommodation, entertainment/media, and commodity exchange. One of the key elements that underpins successful implementations of sharing economy applications, platforms and communities is establishing ways of enhancing trust in the system by various stakeholders. Understanding these trust mechanisms in more detail will be a significant input to the final roadmap produced by this project.

There are a number of areas that would benefit from policy interventions related to the sharing economy:

- **Creating a regulatory environment that promotes growth in sharing economy approaches** at the European level is a key factor. The Digital Single Market offers a potential mechanism to allow European sharing economy entrepreneurs to extend their businesses across borders to better compete with US services that benefit from a larger potential domestic market.
- Building key principles that support a sharing economy into **data protection regulations, European strategies for digitising industries, and rules regulating digital single market exchanges** will be particularly important. Doing so will require the active involvement of sharing economy stakeholders in setting these priorities, since they will bring a different perspective than large established firms.

Research is also needed to better understand the relationship between decentralized sharing economy services and broader societal issues such as consumer protections, licensing and regulation authority, the protection of workers’ rights, and fair models of accounting and taxation.

The medical sector generally and **eHealth** in particular are at an interesting inflection point from a policy perspective. Across many areas of health, there are rapid changes occurring. On the positive side, medical research is advancing at rapid speed particularly related to the decreased costs and increased power associated with genomic research. Funders in Europe and elsewhere have invested heavily in both basic and applied health research, and as a result, we have a much better understanding of the risk factors for illness and protective factors that mitigate these risks. We are also in an era where we are just starting to realize the potential benefits of leveraging massive quantities of health-related data, ranging from bespoke research data through medical records and administrative data all the way to personally generated health data such as ones generated by personal self-tracking devices.

Not everything in the health sector, however, is as positive. Across Europe and globally, the successes we have seen at saving lives and extending lifespans has meant that we have an increasingly aged population that is also associated with increasing health care requirements and cost to provide care for the elderly. Many national health systems are lacking required staff to deal with growing numbers of patients, and funding has often failed to keep up with growing utilisation. In addition, the ubiquity of personal health information raises serious ethical issues that societies have only begun to deal with.

From the analysis in Section 4.2.5, we established that areas for policy intervention include:

- **Privacy and security of health data** is frequently discussed and researched, but additional work is needed to join up the many initiatives in this area to build broader consensus over best practices at all levels
- **Clearer rules for the management of medical data** are needed to reduce uncertainty, both within the health system and for new human-machine configurations that produce health data (e.g. Fitbit) and consume health data (e.g. longitudinal medical research relying on repurposed medical data).
- **Increased clarity in the regulatory environment for eHealth applications** will allow novel applications to be developed by new entrants and experienced players in the health sector while reducing the risk of dangerous applications being offered to the public without any process of professional certification.
- **Development of more reliable network infrastructures** that are needed to support guaranteed quality of service, availability, and low latency required for critical needs such as telesurgery.

More research and innovation is also needed to develop automated machine-based ways to process health-related data while maintaining confidentiality and security. There have been advances in developing ‘safe settings’ that allow access to sensitive health data for qualified parties, but mechanisms that allow machine actions within these safe settings to then be used safely and securely while keeping patient identities private are still in their early stages.

When we speak of **citizen participation**, we refer to higher levels of citizen power that extend beyond tokenism or forms of pseudo-participation that do not result in any true potential for action beyond the individual. Many of the HMNs designed to enhance citizen participation focus on facilitating discussion, enabling negotiation, and providing a platform for sharing content (e.g. social networks or knowledge creation systems).

One of the key ways that HMNs alter the landscape of citizen participation is the increased involvement of machine agents such as bots that are designed to take advantage of increasingly open data sources to mine data, filter and combine information, and share these results with the network. Further, HMNs focused on citizen participation increase the possibility that such networks can scale from the very local (which traditionally represented a frequent form of active citizen participation more active than simply voting) to the regional, national or global scale. Common interests are not necessarily as limited by geography as they once were, and HMNs facilitate exchanges among citizens who wish to participate with others who share their goals.

There are a number of complicating factors which shape the extent to which HMNs are successful at promoting citizen participation, including the limitations of motivation, negotiating the delicate balance among trust, control, transparency, and accountability, and the ability of any system to withstand attempts to subvert it.

Some specific areas for policy intervention with regard to citizen participation are:

- **Strengthening trust in the security of citizen participation networks, and trust in the other stakeholders** with whom the network is engaged. There are technical challenges here related to trust and security, but equally social and organizational issues about trust in the other actors (such as government authorities, partisan organizations, or commercial entities) which can enhance positive deliberative action in the best of scenarios or exploit or subvert the network in the worst of scenarios.
- **Opening network data to all actors** which can encourage the development of additional services and enhance transparency. However, care must be taken that these data are not used in ways that undermine trust in the network.
- **Enhancing participation among under-represented groups** is important if the places of digital engagement are to represent society more broadly and not become digital enclaves for the well-off and well-educated.

Some key research areas thus include researching ways to build better, simpler, and more transparent security systems that allow all stakeholders to not only see the activities of the HMN, but also to trust that the other stakeholders' activities are not being carried out in bad faith. Furthermore, finding better feedback mechanisms that allow participants to see the effects of their own participation in the network will again have the potential of creating a positive feedback loop wherein the recognizable outcomes of previous participation encourage future participation.

Telework is in some ways a precursor (by at least several decades) to the sharing economy, as both are focused on increasingly location-independent styles and modes of work. One important difference between the two is that telework typically is used in more formal organizational contexts. As a result, the policy interventions in this sector are somewhat easier to target, as many organizational players are already subject to well-developed regulatory frameworks.

Telework historically has relied on human-machine networks in which the human agency was high and the machine agency relatively low, relying as it has on simple technologies such as telephony, laptop computers, secure internet access, standard office productivity software, and sometimes video communication. The now decades-old promise of telework to remove geography from work considerations has only been partly realized, as many workers rather than being wholly teleworkers instead use telework to increase flexibility, reduce cost and difficulty associated with excessive commuting, and retain work connections even when life circumstances change.

Policy interventions to support effective and productive telework include:

- **Legislation that will increase worker and employer certainty** about appropriate firm-level policies for compensation, work arrangements, taxation regimes, health and safety, and privacy and personal data protection.
- **Reduction of inequalities** across countries in Europe with regard to uptake of telework-friendly policies that currently contribute to differential access to flexible working arrangements in different countries and sectors, which in turn affects parents with family responsibilities in particular.

- **Collecting and disseminating more complete and reliable statistics about telework** across Europe will help to better understand the true level of telework already happening so that policy interventions can be more effectively targeted in areas of underperformance.

Along with these specific policy interventions, if telework is going to increase, there is also scope for additional technical development of fast and reliable human-machine networks that make telework either more accurately resemble face-to-face interaction, or alternatively generate new augmented forms of interaction that are better than face-to-face.

Workplace robotics as a HMN looks at the ways that robotic systems are automating human tasks, from very simple repetitive tasks to very complex automated systems such as self-driving cars, health care robotics, and drone weapons systems. Unlike some of the other HMNs discussed in this project where we have focused initially on the interaction between the humans and the machines, for many robotic applications, we can focus first on the interaction between the machine and the physical world. These robot-environment interactions may ultimately benefit human actors, but for at least some of them, the attraction of automation is specifically that of removing human actors from the interaction. Human actors may still direct or supervise the actions of the robots, but the robot (in the case of a fully implemented system) will perform the task ultimately.

The technical challenges to implementing a fully autonomous robotic system that is scalable and flexible are non-trivial. Adaptive algorithms are required, and the complexity of these algorithms increases massively as the range of environments within which the robot must respond increases. Thus, if robots are to be successfully integrated into social environments (as opposed to tightly controlled assembly-line facilities, for instance), they must react to environmental stimuli, to humans and human behaviour, and to other robots.

There are currently large investments into developing more capable robotic systems. However, it is important to couple these investments with appropriate policy considerations, including:

- **Explicit consideration of ethics in HRI research, development and marketing**. Human autonomy, bodily and mental integrity, and protection of human rights should be a fundamental aspect of new robotic developments.
- **Legal frameworks are needed** to deal with unresolved issues of liability, insurance, data protection, security, and the regulation of potential robotically enhanced human capabilities.
- At a societal level, broader discussions that address **the types of labour that can and should be carried out by robots** (and conversely, those that should not be) are needed. These discussions should take place at a technical level, but also should take into account broader societal questions about employment and jobs more generally, as well as deep questions about inequality and equal access to the benefits of automation.

The technical research possibilities related to robotic automation of tasks and work are vast. We would argue, however, that these developments also need to be joined with research into legal, ethical, and society consequences of robotic labour.

Decision support systems (DSS) for crowd management focuses on the ability of automated and semi-automated systems that can both *monitor* the activities of crowds, and when such monitoring identifies incidents, to more actively *manage* the response of the crowds and of other actors (which might include emergency and/or security personnel) to the incident.

One of the traditional limitations of simple monitoring systems has emerged when human operators ignored or overrode warning systems that were not engineered in ways that provided adequate trust in the systems. Some highly publicized disasters or near-disasters were in situations where monitoring equipment should have allowed monitoring personnel to respond to a developing situation, but did not do so for a variety of reasons. HMN-capable crowd management DSS, on the other hand, are designed to increase trust in the system by all actors involved and to minimize harm to the actors while responding to the crisis situation.

One of the most obvious differences between such systems and the other types of HMNs that we have discussed is that there are two radically different dynamical states that must be catered for. During the monitoring phase, many of the human actors (those in the crowd) will be largely passive creators of data that are feeding into the system. Machines and a small number of humans will be actively monitoring the crowd, but this monitoring will take place nearly or completely invisibly to the majority of actors. When a crisis occurs, however, the entire system becomes much more visible by its actions (or, in the case of failure, by inaction) coordinating human and machine responses to the crisis.

Key policy interventions for these systems include:

- **Establishing a norm that policies related to crowd monitoring and response considers all actors** when designing systems and establishing regulations for their use. Future policy for decision support systems must include all network players, and not simply machines or official agencies.
- **Openness** should underlie coordination and communication to enhance the management of crisis situations and increase the ability of actors within these situations to shape their own response based on clear and unambiguous information and knowledge of what other actors are doing.
- **Ensuring that responsibility resides with human actors** and that actors making final decisions are knowledgeable about the strengths and limitations of the HMN so that decisions are made based on the most complete knowledge available.
- **Establishing clear mechanisms for coordinating human actors that result in cooperative responses** and limit destructive responses based on social categorizations.

Research challenges related to the use of decision support systems for crown management exist at both the technical level and the social level. From the technical point of view, research is needed to increase the robustness and reliability of monitoring and response systems, and their flexibility. At the social level, additional research is needed into crowd behaviour in different situations, and particularly it should move beyond the erroneous stereotype of the panicking crowd. Further, ethical and legal issues must be clarified to protect both the rights of individual and the work of monitoring staff and response personnel.

Across all the cases, we can see that several themes are recurrent: the need for a **better understanding of the ethical issues** raised by tighter integration of humans and machines, the need for **more privacy**

and policies that address the close relationship amongst openness, privacy, and trust, and the need to take an ecosystem view that includes **all human and non-human actors both when designing systems and when writing regulations.** All of these speak to a fundamental need in the area of HMNs, which is that **more clarity** is needed in the policy arena if these systems are to reach their potential to enhance human potential and quality of life.

7 Conclusion and further work

In this deliverable we have identified some important implications in HMNs that can affect and transform norms of behavior in different social domains such as health, economy, work, governance. We have also identified technical and non-technical challenges and policy interventions that could be applied in each domain, so that machines are integrated harmoniously in human life, but also humans adapt to certain machine behaviors and outputs. We have identified the main stakeholders in each domain whom we intend to engage in roadmap development and provide with channels of cross-communication, so that there fruitful exchanges between stakeholder categories.

This collaborative effort will improve the roadmap that we will build in the next steps. The development of the roadmap will be a living process where stakeholders from the different domains will be consulted to further analyse and validate the roadmap goals, the process to achieve the goals, concrete actions and their expected outcomes.

Roadmaps will be constructed for several of the social domains presented in this deliverable. Our goal is to present mini-roadmaps focusing on single domains and one or more HMN applications (since some domains, such as eHealth contain more than one distinct HMNs), identifying challenges and policy interventions, specifying goals, stakeholder actions, and a time plan for accomplishing the goals. Despite the fact that HMNs in different domains may share some common challenges and objectives, we will design separate roadmaps for each domain, in order to manage and evaluate them more efficiently.

The work done in this deliverable is an initial attempt at understanding HMN challenges, opportunities, and needs for future thinking in these domains, and will be finalized during roadmap development. In addition, the HUMANE method and tools (D2.2) will have a central role in designing the roadmap, as they can readily provide design patterns based on the characteristics of the HMN and provide examples of similar networks, in order to choose the most efficient technology solutions. There is also a link between regulations and design patterns. So, a policy maker could see that a regulation should be improved or changed in order for a design patter to be implemented.

More specifically, a HUMANE roadmap will be a document consisting of: a) the current technological situation, policy background and regulatory context, b) the goals and expected outputs of the roadmap, c) the required actions to achieve the goals, d) design patterns and technology solutions (drawing on input from D2.2), e) breakdown of the roles of stakeholders and f) implementation priorities and timetable. The roadmaps will be developed by carrying out desk research, consulting the stakeholders and will be published and presented to the wider community of each social domain.

8 References

Acquisti, A. (2012). Nudging privacy: The behavioral economics of personal information. In *Digital Enlightenment Yearbook 2012* (pp. 193–197). http://doi.org/10.3233/978-1-61499-057-4-193

Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems*, *36*(1), 93–101. http://doi.org/10.1007/s10916-010-9449-4

Andrew Bagnell, J. (2014). Reinforcement Learning in Robotics: A Survey. *Springer Tracts in Advanced Robotics*, *97*, 9–67. http://doi.org/10.1007/978-3-319-03194-1_2

Ball, M. J., Smith, C., & Bakalar, R. S. (2007). Personal health records: empowering consumers. *Journal Of Healthcare Information Management: JHIM*, *21*(1), 76–86.

Blake, S. J., Galea, E. R., Westend, H. and Dixon, A. J. P. (2004). An analysis of human behaviour during the World Trade Center disaster of 11 September 2001 based on published survivor. In *Third International Symposium on Human Behaviour in Fire*.

Botsman, R. (2013). The sharing economy lacks a shared definition. *Fast Company*, 1–8. http://doi.org/http://www.fastcoexist.com/3022028/the-sharing-economy-lacks-a-shared-definition#10

Botsman, R., & Rogers, R. (2010). *What's Mine Is Yours - How Collaborative Consumption is Changing the Way we live*. *Business*. http://doi.org/10.1016/S0168-9525(00)00086-X

Cath Sullivan. (2003). What's in a name? Definitions and conceptualisations of teleworking and homeworking. *New Technology, Work and Employment*, *18*(3), 158–165.

Challenger, R., Clegg, C. W., & Robinson, M. A. (2009). *Understanding crowd behaviours: Guidance and lessons identified*. *Understanding Crowd Behaviours*. http://doi.org/ISBN 978-1-874321-20-0

Davis, M. C., Challenger, R., Jayewardene, D. N. W., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics*, *45*(2 PA), 171–180. http://doi.org/10.1016/j.apergo.2013.02.009

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance - An empirical investigation. *Journal of Strategic Information Systems*, *17*(3), 214–233. http://doi.org/10.1016/j.jsis.2007.09.002

Drury, J., & Reicher, S. (2000). Collective action and psychological change: The emergence of new social identities. *British Journal of Social Psychology*, *39*(4), 579–604. http://doi.org/10.1348/014466600164642

Fahy, R. F. and Proulx, G. (2002). A comparison of the 1993 and 2001 evacuations of the World Trade Center. In *2002 Fire Risk and Hazard Assessment Symposium* (pp. 111–117).

Franco, Z., & Zimbardo, P. (2006). The Banality of Heroism. *Greater Good*. http://doi.org/10.1162/016228800560381

Gianpaolo Cugola, A. M. (2012). Processing flows of information: From data stream to complex event processing. *ACM Computing Surveys*, *44*(3).

Glas, D. F., Satake, S., Ferreri, F., Kanda, T., Ishiguro, H., & Hagita, N. (2013). The Network Robot System: Enabling Social Human-Robot Interaction in Public Spaces. *Journal of Human-Robot Interaction*, *1*(2), 5–32. http://doi.org/10.5898/JHRI.1.2.Glas

Hamari, J., Sj??klint, M., & Ukkonen, A. (2016). The sharing economy: Why people participate in collaborative consumption. *Journal of the Association for Information Science and Technology*, *67*(9), 2047–2059. http://doi.org/10.1002/asi.23552

Helbing, D., Johansson, A., & Al-Abideen, H. Z. (2007). Dynamics of crowd disasters: An empirical study. *Physical Review E - Statistical, Nonlinear, and Soft Matter Physics*, *75*(4). http://doi.org/10.1103/PhysRevE.75.046109

Hoc, J. M. (2000). From human-machine interaction to human-machine cooperation. *Ergonomics*, *43*(7), 833–843. http://doi.org/10.1080/001401300409044

Hynes, M. (2014). Telework Isn???t working: A policy review. *Economic and Social Review*, *45*(4), 579–602.

Jackson, P. J., & Wielen, J. van der. (1998). *Teleworking : international perspectives : from telecommuting to the virtual organisation*. *The management of technology and innovation*. Retrieved from http://www.loc.gov/catdir/enhancements/fy0649/97028677-d.html

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59–68. http://doi.org/10.1016/j.bushor.2009.09.003

Law, J., & Smullen, J. (2014). *A Dictionary of Finance and Banking*. *Oxford University Press*. http://doi.org/10.1093/acref/9780199664931.013.3137

Leone, F. Lavigne, R. Paris, J-C. Denain, F. V. (2011). A spatial analysis of the December 26th, 2004 tsunami-induced damages: Lessons learned for a better risk assessment integrating buildings vulnerability. *Applied Geography*, *31*(1), 363–375.

Levine, M., Prosser, A., Evans, D., & Reicher, S. (2005). Identity and emergency intervention: how social group membership and inclusiveness of group boundaries shape helping behavior. *Personality & Social Psychology Bulletin*, *31*(4), 443–53. http://doi.org/10.1177/0146167204271651

Lipscy, P. Y., Kushida, K. E., & Incerti, T. (2013). The fukushima disaster and Japan’s nuclear plant vulnerability in comparative perspective. *Environmental Science and Technology*. http://doi.org/10.1021/es4004813

Lymberis, a, & Dittmar, a. (2007). Advanced Wearable Health Systems and Applications - Research and Development Efforts in the European Union. *Engineering in Medicine and Biology Magazine, IEEE*, *26*(3), 29–33. http://doi.org/10.1109/MEMB.2007.364926

Makarenko, A., Kaupp, T., Grocholsky, B., & Durrant-Whyte, H. (2003). Human-robot interactions in active sensor networks. In *Proceedings of IEEE International Symposium on Computational Intelligence in Robotics and Automation, CIRA* (Vol. 1, pp. 247–252). http://doi.org/10.1109/CIRA.2003.1222097

MORI, N., & TAKAHASHI, T. (2012). Nationwide Post Event Survey and Analysis of the 2011 Tohoku Earthquake Tsunami. *Coastal Engineering Journal*, *54*(1), 1250001. http://doi.org/10.1142/S0578563412500015

Noggerath, J., Geller, R., & Gusiakov, V. (2011). Fukushima: The myth of safety, the reality of geoscience. *Bulletin of the Atomic Scientists*, *67*(5), 37–46. http://doi.org/10.1177/0096340211421607

Norman, D. A. (2011). *Living with Complexity*. *MIT Press, Cambridge, Massachusetts*. http://doi.org/citeulike-article-id:8527494

Pichler, M., Hofer, T., & Leonhartsberger, G. (2002). Considerations and requirements for tools supporting mobile teams. *22nd International Conference on Distributed Computing Systems Workshop, Proceedings*, 389–390. http://doi.org/10.1109/ICDCSW.2002.1030800

R. Kelly Garrett, J. N. D. (2007). Which Telework? Defining and Testing a Taxonomy of Technology-Mediated Work at a Distance. *Social Science Computer Review*, *25*(1), 27–47.

Riek, L. D., & Howard, D. (2014). A Code of Ethics for the Human-Robot Interaction Profession. *We Robot Conference*, 1–10.

Scraton, P. (1999). Policing with contempt: the degrading of truth and denial of justice in the aftermath of the Hillsborough disaster. *Journal of Law and Society*, *26*(3), 273–297. http://doi.org/10.1111/1467-6478.00126

Strunz, G., Post, J., Zosseder, K., Wegscheider, S., M??ck, M., Riedlinger, T., … Muhari, A. (2011). Tsunami risk assessment in Indonesia. *Natural Hazards and Earth System Science*, *11*(1), 67–82. http://doi.org/10.5194/nhess-11-67-2011

Tajfel, H., & Turner, J. (1979). An Integrative Theory of Intergroup Conflict. *The Social Psychology of Intergroup Relations*. http://doi.org/10.1016/S0065-2601(05)37005-5

Waddington, P. a. J. (2012). Reicher, S. and C. Stott (2011). MAD MOBS AND ENGLISHMEN? MYTHS AND REALITIES OF THE 2011 RIOTS. *Policing*, *6*(2), 221–224. http://doi.org/10.1093/police/pas014

Waegemann CP. (1996). The five levels of electronic health records. *MD Computing*, *13*(3), 199–203.

William Form. (1987). On the degradation of skills. *Annual Review of Sociology*, *13*(10), 29–47.