European Commission

JRC SCIENCE AND POLICY REPORTS

Emerging ICT for Citizens' Veillance

Theoretical and Practical Insights

Mariachiara Tallacchini
Philip Boucher
Susana Nascimento

2014

Joint Research Centre

Report EUR 26809 EN

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
TALLACCHINI Mariachiara

Address: Joint Research Centre, Via Enrico Fermi 2749, TP 361, 21027 Ispra (VA), Italy
E-mail: mariachiara.tallacchini@jrc.ec.europa.eu
Tel.: +39 0332 78 9746

https://ec.europa.eu/jrc

JRC 90334

EUR 26809 EN

ISBN 978-92-79-39775-2

ISSN 1831-9424

doi: 10.2788/11828

Luxembourg: Publications Office of the European Union, 2014

Abstract
The report explores theories and practices surrounding citizens' veillance activities, namely a broad range of citizen-driven initiatives for civic purposes. These can aim at creating new forms of knowledge and awareness; building new social communities and commitments; contributing to protection of common goods; empowering citizens in protecting or restoring some fundamental individual and collective rights. The concept of "veillance" is used here to refer to activities performed by citizens broadly and primarily to produce socially useful, empowering knowledge —rather than to control somebody. Therefore, the working definition proposed for veillance is a condition of citizens' cognitive alertness and knowledge production proactively oriented towards the protection of common goods. Describing the workshop on Citizens' veillance held on 20-21 March 2014 at the JRC in Ispra, the report further elaborates these discussions and reflections by providing some provisional recommendations while identifying several epistemic and normative issues emerged that require further investigation. Several ongoing changes are reframing the processes of knowledge production. Science and knowledge are no longer produced only in official sites, but everywhere in society, and especially through ICT and the web. Scientists' (and artists-scientists') and citizens' science often merge and converge in producing relevant, reliable and transparent knowledge to complement and in some instances change or redirect official, institutional knowledge. In order to be democratically legitimate and to re-draw the boundaries between the traditional public function of knowledge production and these new forms of lay production of knowledge, the values promoted by these initiatives are to be reflected in more democratic and transparent ICT architectures.

Contents

1. Summary

In ubiquitous surveillance societies, individuals are observed and controlled by authorities, institutions, and others. Some participatory approaches involve citizens contributing their tech-knowledge to their own surveillance. Moreover, the watched are also observing the watchers through sou-veillant activities, often aiming to control the kind of knowledge that is produced and whether powers are implemented within legitimate limits.

However, existing and emerging ICT are increasingly used for bottom-up initiatives where citizens define the goals, shape the outcomes, and profit from the benefits of watching activities. This model of citizens' vigilance, or veillance, may present opportunities for individuals and collectives to be more prepared to meet the challenges they face in various domains including environment, health, planning and emergency response.

The concept of "veillance" is used here to refer to activities performed by citizens broadly and primarily to produce socially useful, empowering knowledge —rather than as a means of control. Therefore, the working definition proposed for veillance is a condition of citizens' cognitive alertness and knowledge production being proactively oriented towards the protection of common goods.

Several epistemic and normative issues emerge and require further investigation.

From the epistemic point of view, we are looking at the changes that have taken place, and are taking place, in the processes of knowledge production. Science and knowledge are no longer produced only in official sites, but everywhere in society, and especially through ICT and the web. Scientists' (and artists-scientists') and citizens' science often merge and converge in producing relevant, reliable and transparent knowledge to complement and in some instances change or redirect official, institutional knowledge. Different forms of knowledge, technical tools, and skills have merged in community-based scientific and social endeavours through ICT as powerful ways to gain more control over their health and the environment.

Moreover, from both an epistemic and normative stance, knowledge is collectively peer-generated and produced by means of individually accessible and usable, and in many cases Do-It-Yourself (DIY) ICT. In order to be democratically legitimate and to re-draw the boundaries between the traditional public function of knowledge production and these new forms of lay production of knowledge, the social (perhaps constitutional) values promoted by these initiatives should be reflected in more democratic and transparent ICT architectures.

From the normative perspective, we wish to explore situations where knowledge production through ICT aims to protect common goods —such as health or the

environment— and often to prevent potential infringement of rights, or to restore them. Health and the environment represent two major historical domains and social —and in several countries constitutionally protected— values where civic and community activities have taken place even before the wide availability of ICT empowered citizens to create knowledge and awareness and to share data and results.

However, not all ICT are alike: the technologies used to perform these initiatives range from web platforms to portable and wearable sensors, to drones and open source surveillance and mapping kits. The requirements for these technologies as to their accessibility, usability, degree of invasiveness and pervasiveness, criteria for openness and transparency are diverse and complex.

The main questions we are asking are: how are these new forms of peer-production or citizens-led production of knowledge redefining the boundaries between public and private knowledge production (e.g. in their policy and legal use)? How should ICT be designed to reflect the goals promoted by these activities, and how values- and rights-in-design should be embodied in ICT architectures and made accessible and available to citizens/users? Who will be the main contributors in defining the relevant values and rights, and through which processes authorities, policymakers, industry, civil society organizations, users, and communities can interact and intervene in ICT orientation? Which are the main challenges arising from the use of DIY and open source tools in order to empower citizens and communities not only to create and share data in a collaborative logic, but also to provoke transformations in their practices?

The JRC workshop on "Emerging ICT for Citizens' Veillance" was held on March 20-21, 2014 in Ispra (agenda presented in Annex 1). The aim was to explore the broad range of activities that are simultaneously creating new forms of knowledge and awareness; building new social communities and commitments; contributing to protection of common goods; empowering citizens in protecting or restoring some fundamental individual and collective rights. The workshop brought together scholars, technicians, policy-makers, and activists to consider how emerging ICT can be designed to reflect citizens' values and to support citizens' empowerment in democratic, affordable, and sustainable ways. Through presentations and roundtable discussions, participants discussed the current state-of-art and existing experiences with emerging ICT in relation to citizens' vigilance and consider ethical questions, potential technological solutions and future research topics.

The workshop was composed of three sessions: the first was focused upon theoretical aspects, ranging from deeper visions of privacy to the policy and ethical issues surrounding surveillance technologies. The second session explored these issues with reference to practitioners' experiences with technologies. This session was split into two parts: Part I focusing upon the experiences of two research groups on

environmental protection and monitoring, and Part II dealing with a prominent theme for veillance technologies—health and bodies. In the third session, we explored how veillance technologies presented opportunities for DIY and open source projects that articulate new visions and ways of visioning.

The workshop was part of the JRC Project 'Trust in Digital Interactions: Citizens, Institutional and Corporate Ethics' (TRUDI, Project n. 568). TRUDI deals with "research on ethical approaches for improving trusted digital interactions. Nurturing trust requires multi-layered, technical and non-technical ways of interweaving the social digital fabric: institutional ethics and digital memories, organized citizens' vigilance to support corporate responsibility, international data sharing." The goal of the project is to understand what trust means when most interactions between citizens and institutions are digitalized and what is needed to establish trusted relations in the so-called virtual, but already very real world.

While the workshop explored some theoretical and experiential dimensions, the aims of this report are to present the major elements that emerged during the meeting and, furthermore, offer some recommendations for best practices in citizens' veillance as well as indications for further analysis.

2. Introduction: from surveillance to veillance

2.1 The contemporary multiple imaginaries for surveillance

The modern imaginaries about technologies of surveillance are well known to be inseparable from top-down visions of power and control: from Bentham to Foucault, the Panopticon has represented the default image of this all-devouring gaze. Subjects are reduced to objects as they are forced to internalize the external power by self-disciplining their conducts (Foucault 1975).

Moreover, surveillance has always posed delicate ethical issues (Burke 2007), as it has been mostly framed not just as a means of granting security, but as an end in itself; and it has covered the power of sovereign States to suspend or limit citizens' rights for security reasons by invoking "states of exception" (Agamben 2006).

Traditionally, surveillance refers to a hierarchical system of power, with the gaze of the watcher controlling the watched. The watched is reduced to a passive subject, mostly disempowered by the real or imagined presence of the gaze: "…to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power" (Foucault 1995:195). David Lyon has defined surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon 2007:14). Typically, surveillance refers to activities enabling governments or corporations to manage a population. Also, this conception of surveillance involves an asymmetry in power as one characterizing institutions and superindividual entities.

Traditional surveillance has developed from the religious to the State surveillance in the modern age, and has then moved towards a broadly "policed" society, to a bureaucratic collection of personal information for various law and rights enforcement purposes, to surveillance for social planning and in relation to the welfare state as well as in public health activities. The same dynamics of consumerism are inconceivable without the massive collection of personal data.

The ubiquitous presence of electronic eyes in contemporary societies has ambiguously changed this gaze. While the Panopticon's "big single gaze" has faded away, a kaleidoscope of massive, distributed, and inexpensive technological "eyes," from sensors to mobiles to drones, [1] has colonized sparse, interconnected fragments of personal and social lives. Public and private spaces cannot be sharply separated any more, but have blurred into a continuum.[2]

---

[1] See, for instance, Do-It-Yourself Drones, http://diydrones.com/ , and http://www.meetup.com/DC-Area-Drone-User-Group/, defined as "a group for amateur and professional drone users committed to promoting the use of flying robots for recreational, humanitarian, and artistic purposes" (Accessed 13 May 2013).

[2] See, for instance, the European Court of Human Rights case *Peck V. United Kingdom* (2003) 36 E.H.R.R. 41.

Surveillance is no longer just visual. Indeed a variety of devices capable of storing all kind of information can be perceived as metaphorical "eyes" that cover everything from the external environment to the internal genetic make-up.

The massive availability of inexpensive ICT devices, from wearable sensors to smart phones to social network platforms, has radically altered this big single gaze: by fragmenting and multiplying it into a kaleidoscope of ubiquitous technological 'eyes' colonizing public and private spaces; by introducing a more horizontal dimension to the vertical; by de-coupling the source of information from visual surveillance. Even though State surveillance has only become stronger, more pervasive and networked and more diversified as to the means applied (as recent surveillance activities in the US have shown), the changes brought about by new forms of 'lateral' surveillance enabled through individually usable technology are also ambiguous.

Although individuals are supposed to be trapped primarily by the gaze and unable to escape its pressure, traditionally, forms of resistance to surveillance have been developed. The concept of what has been called 'sousveillance' (Mann, Nolan, and Wellman 2003), namely surveilling from below, has been applied to situations where the weakest part of a relation/interaction has the chance to redirect the gaze back, thus producing an inverse surveillance: watching the watchers.

All these changes have been the object of surveillance studies for more than a decade, revealing continuities and new dynamics. In 2002, Gary Marx, the founder of Surveillance & Society, described 28 different dimensions for new surveillance that have emerged in the last part of the 20th century, and that are partly innovative and that partly derive from traditional surveillance (Marx 2002). The definition of new surveillance proposed by Marx is "the use of technical means to extract or create personal data," where 'technical means' "implies the ability to go beyond what is offered to the unaided senses or is voluntarily reported," and "excludes the routine, non-technological surveillance that is a part of everyday life" (Marx 2002, 12).

First of all, the means through which surveillance can take place have completely superseded the visual reference, to explode in a variety of heterogeneous, and often portable and wearable, sensors. Hearing, touching, smelling, as well as measuring, associating, and predicting have all become part of the "visual." All data, from biology to biography, can enter the picture, while "seeing" increasingly assumes the meaning of "seeing through" (Marx 2002), seeing forward, and making forecasts.

Second, the actors involved are not only States and corporations, but all individuals. Everybody can perform surveillance on everybody else and can be observed. The increasingly microscopic dimensions of tools (from glasses to drones) can make the

activities partially or completely undetectable, and in many ways the awareness of being constantly observed has become an almost normal(ized) feeling.
Moreover, a third prominent character for new surveillance is a "general ethos of self-surveillance," already described by Foucault as a form of care for the self, but that in recent decades has amounted to another form of social control (Vaz and Bruno 2003).

According, again, to Marx, self-surveillance has blurred the line between the surveilled and the surveillant (Marx 2002). It can be added that not only the surveillant looks at the self as a detached and detachable object of control, but also that the self-surveillant can comply with, and submit to, more traditional forms of surveillance and surveillants. These practices have been encouraged by the large availability of home testing products (from blood sugar to pregnancy), including DTCs genetic tests – though these require a third party capable of interpreting the results. Now smartphones can store and elaborate most health information and deliver plans for a healthier life (Jacobs 2012). At the same time these self-monitored activities acquire a mandatory aspect by becoming specific expectations for responsible behavior.

The privatization of surveillance that can be individually and reciprocally performed in increasingly unnoticeable ways is radically transforming the issue of the legitimate uses of these technologies. Together with sovereign States, corporations, groups, and individuals can now intrude in all aspects of life. All these unleashed powers need to be rethought in order to assess and balance them, to harmonize them with fundamental rights, and to ground them in more robust forms of democratic legitimacy.

2.2 Participatory surveillance

An additional characteristic of contemporary surveillance is "participation" in surveillance, namely the involvement of a plurality of heterogeneous subjects as agents of surveillance, and the resulting ambiguous boundaries between voluntary and involuntary surveillance. This new feature implies that, in order to understand it as a dynamic process, surveillance has to be examined in the light of the power relations and the social relations that it produces (Fernandez and Huey 2009, 199). "Mandatory volunteerism" is the expression used by Marx to refer to the broad phenomenon of "requesting volunteers based on appeals to good citizenship or patriotism; using disingenuous communication; profiling based on life style and consumption; and utilizing hidden or low visibility information collection techniques" (Marx 2006).

As Florian Henckel von Donnersmarck has shown in "The Lives of Others" (2007), these disguised forms of "voluntarily" participation in surveillance are not new. However, the softer and less invasive quality of current surveillance techniques has contributed to a blurring of the lines between full and an attenuated awareness of providing information to a third party, and the idea that even uninformed data collection can be seen as participation in surveillance.

"In the convoluted logic of those who justify covert (or non-informed) data collection and use, individuals "volunteer" their data by walking or driving on public streets or entering a shopping mall, by failing to hide their faces or wear gloves or encrypt their communications, or by choosing to use a phone, computer, or a credit card" (Marx 2007, 15).
The very idea of participatory surveillance has been framed in different ways and given different meanings, with surveillance merging with self-surveillance, and with various degrees of (un)intended contribution to surveillance . According to Albrechtslund (2008) the concept of "participatory surveillance" has been used (for the first time in 1990 by Mark Poster) to argue that today's circuits of communication and databases constitute a superpanopticon. In this perspective individuals are not just disciplined, but take active part in their own surveillance, even more by continuously contributing with information to databases. In a similar way, Cascio has coined the expression "participatory panopticon" to describe the situation where "constant surveillance is done by the citizens themselves, and is done by choice, …the emergent result of myriad independent rational decisions, a bottom-up version of the constantly watched society" (Cascio 2005).

The unruly, disordered way of referring to participation to describe the multiform crowds of contributors to the dynamics of surveillance has grown in ambiguity, partly due to the unconditional value assigned by contemporary democracy to participatory procedures. Framing surveillance as participatory has been a formula to suggest its democratized character, and to distract attention from the actual subjects empowered by surveillance and from their goals: who is in control of them and which these are.
If citizens' collaboration with the power has only partially reframed the meaning of surveillance, as far as citizens' trust is taken for granted without them to be made properly aware of the purposes or potential secondary uses of the data they are asked to provide, that remain largely unverified by citizens/participants.

Not all forms of participation are alike, and the mere participatory nature of surveillance does not justify its overall legitimacy. The need to rethink the reasons, the means, and the ends for performing surveillance concerns institutions, corporations, and individuals. While the appeal to State security—historically representing the most accepted rhetoric for surveillance (House of Lords 2009)—is perceived as increasingly controversial in its indiscriminate application, and while surveillance over consumers requires some warrants and limits as well, monitoring performed by citizens should also meet some criteria for legitimacy.

2.3 Citizens' veillance as a legitimate practice in democratic societies: epistemic and normative dimensions

Participation per se is not a significant sign of a paradigm change in surveillance if the powers involved are not re-considered, re-balanced, and re-legitimized. In this respect

the simple addition of a participatory dimension to surveillance neither implies that its goals are disclosed to, known and controlled by participants, nor that they can be justified in terms of the constitutional values and rights which inform society. A different category of cognitive practices for social intervention requires more attentive consideration as to the powers, the rights, the means, and the goals involved. A paradigm shift is required to ensure that surveillance activities are framed and performed while respecting all participants' rights through legitimate technological means, and for the protection of (uncontroversial) common goods and socially legitimate—perhaps constitutionally established—goals.
The concept of citizens' veillance is introduced to explore initiatives and practices where these requirements are met. The idea is used here to refer to activities performed by citizens broadly and primarily to produce socially useful, empowering knowledge —rather than to control somebody. Therefore, the working definition proposed for veillance is a condition of citizens' cognitive alertness and knowledge production proactively oriented towards the protection of common goods.

The reasons to suggest the term veillance are manifold. First, the elimination of the locations and directions of the inquisitive "gaze"—the sur- sous- and also self—aims to turn the "watching somebody or something" into a broader "becoming aware" of the surrounding context; and to propose a shift from control to cognition, from power to alertness. Also the Hannah Arendt's famous term "vigilance" would not be properly applied here as it was introduced mostly to refer to a lack of moral awareness, to the perils of being blind towards the consequences of our acts, and therefore to the need of constantly morally checking on ourselves. If, indeed, an element of vigilance is implied in the activities defined here as citizens' veillance, there are more dimensions that both are foreign and go beyond the idea of vigilance.

These further elements consist of the collective production of knowledge that these activities aim to generate; of the practical, social destination of the knowledge endeavor, and more specifically of the proactive protection of some fundamental rights and values.
The empowerment gained through veillance activities may result in creating more robust knowledge that can complement, implement, and sometime confront institutional or corporate knowledge production. For instance, populations living in highly polluted sites started self-monitoring of their environment and health conditions in order to confront the scientific evidence presented by industry; in Corporate Social Responsibility, citizens can provide their experience of corporate behaviors as an indirect form of control of self-declared good practices. In other experiences, individuals and communities become empowered for themselves and/or for the benefit of others. Examples include communities concerned about the spreading of infectious diseases in potentially affected areas performing early detection of cases and symptoms, [3] communities living in areas susceptible to natural

[3] http://healthmap.org/en/ (Accessed 14 May 2013).

disasters raising their alertness towards preparedness and limiting damages, and communities of people with chronic disease conditionsmonitoring each other to generate more freedom and safety (Weitzmann et al. 2013).

In each of these cases, the general framework for alertness and knowledge is oriented towards more democratically-shared and controllable goals; it is conceived for, and legitimized by, the benefit of communities; and it represents a strategy for improved protection of citizens' rights.[4]

Moreover, this paradigm shift is coherent with the concept of security endorsed by critical studies as it is moving towards an emancipated normativity, with security and surveillance disentangled from power.

However, some epistemic and normative requirements are required to identify and develop best practices for citizens' veillance. Indeed, the ways knowledge is produced and the technologies involved have to be consistent with the normative attempt to respect rights and protect common goods. On the epistemic side, there is a need for the technologies that are used to be open, accessible, and transparent. On the normative side, the veillance activities have to be legitimate with regard to their ends and means. From this perspective, in the following two paragraphs some epistemic and normative requirements are explored.

2.3.1 Opening up ICT for veillance: DIY and maker approaches, and rights in-design

Many designers of citizens' veillance systems face a common issue in the degree of openness of the digital architectures and ICT involved in citizens' veillance.

Frequent requirements of citizen-led activities include: Open source software and platforms that can be freely adopted and modified; the creation of structures providing access to open, and even raw, reusable data; the transparent character of all procedures; the sharing of data together with adequate forms of embedded protection of privacy and personal data (privacy by-design); the possibility to intervene in the design and to modify it (rights in-design); and the preference for Do-It-Yourself (DIY) approaches. Moreover, these technological requirements are now increasingly coupled with specific open forms of funding, namely crowdfunding, as the economic counterpart of the independency and trustworthiness of a proposed initiative.

While some of these requirements and the philosophy that they endorse are well-known—e.g. open source programme—others, such as the DIY approach and rights in-design—are less debated and their potential for more open and democratic approach to technology is not well-established. We would like to draw attention to these two features as relevant elements for citizens' veillance activities.

[4] See the journal Surveillance & Society 2011, http://www.surveillance-and-society.org/ (Accessed 14 May 2013).

DIY and maker approaches

DIY approaches, broadly referring to activities of creating, modifying or repairing artifacts by one's initiative or without 'professional' or 'expert' assistance, are merging with new realities of making, fabbing [5] and tinkering, which are seen to support more decentralized and collaborative engagements with technology. On one hand, a diversified set of tools and machines are becoming more accessible for a wider range of users/citizens/groups/communities to design, manufacture and produce artifacts (objects, systems, networks or applications), such as digital fabrication devices (CNC machines, CAD programs, laser cutters, 3D printers), open source and low-cost hardware (Arduino, Raspberry Pi, and others), ambient sensors (for instance Co2, temperature, light intensity, sound, or humidity), or even smartphones and smart devices. On the other hand, the relevance of such technologies is to be understood within an online availability of data and documentation for conducting your own projects, such as schematics, circuit layout, code, 3D models, electronics tutorials and support materials, and very importantly, in the context of online communities exchanging experiences, sharing their work, and connecting with and supporting others with common interests.

In the past few years, we have been witnessing the rise of DIY and making approaches, which are calling for more and more people to open up their devices, personalize them, hack them, mash them up, understand and affect their inner workings, and create new ones. Individual and collective actors are coming into play, from crafters, hackers, artists, designers, scientists and engineers, to amateurs, hobbyists, entrepreneurs, companies, students, professors, researchers, children, communities, and civil society organizations. They are modifying and creating things on their own in a more traditional idea of DIY, but mostly Doing-It-Together (DIT) or Doing-It-With-Others (DIWO), at local and global levels, in their homes, garages, schools, science museums, libraries, FabLabs, Makerspaces, Hackerspaces, Techshops, [6] or other types of innovation labs. [7]

For the most part, present maker discourses and practices are oriented towards the values of self-expression, knowledge sharing, community building, re-skilling, creativity, and innovation. It is more popularly visible in bold proclamations of 'we are all born makers' (Anderson, 2012), or '(almost) anybody can make (almost) anything' (Gershenfeld 2007), or in 'maker manifestos' (Hatch 2014) focused on buzzwords of

[5] Fabbing refers to activities of digital fabrication, that is, manufacturing processes that use computer-controlled machines, such as CNC milling machines, 3D printers or laser cutters.

[6] FabLabs, Makerspaces, Hackerspaces or Techshops cover a number of spaces offering access to digital fabrication, electronics and other ICT tools for rapid prototyping, under a common rationale that any user, consumer, or citizen can be ultimately able to produce, use, share, copy and improve objects, systems or devices.

[7] An Innovation Lab can be, for instance, "a space and set of protocols for engaging young people, technologists, private sector, and civil society in problem-solving" (UNICEF, 2012. Innovation Labs: A Do-It-Yourself Guide, http://www.unicefinnovationlabs.org/?page_id=463, accessed 20 August 2014)

"make, share, give, learn, tool up, play, participate, support, change", or in 'Maker's Bill of Rights' [8] or the '10 Commandments of Making' [9] held by Make Magazine, also the publisher of several books on these issues and the organizer of the Maker Faire.

Its disruptive impact is becoming visible, in terms of not only cultural relevance and popularity, but also economic and political significance. In terms of economic importance, a recent report [10] gives an overview of this next generation of craftspeople, tinkerers, hobbyists and inventors, who are experimenting with new fabrication tools and forming communities that are reshaping the meaning and ways of doing technological innovation. Quoting this report, "making – the next generation of inventing and do-it-yourself – is creeping into everyday discourse, with the emerging maker movement referenced in connection with topics ranging from the rebirth of manufacturing to job skills development to reconnecting with our roots."

As for political significance, already in his November 2009 speech for the "Education to Innovate" Campaign, President Obama talked about "the promise of being the makers of things and not just the consumers of things," [11] referring to his commitment to STEM education. Moreover, President Obama proclaimed June 18 as the National Day of Making [12] in the opening of the White House Maker Faire, thus strengthening US commitment to 'democratization of technology' through sparking creativity and stimulating innovation in each community.

In an interview at TEDx Brussels in October 2013 [13] Commissioner Kroes acknowledged the emergence of new peer-to-peer economies and that "joining and sharing is the thumb rule of the new economy." The political importance of these trends is also visible in the initiative Europe Code Week, focused on stimulating 'digital skills'. It is particularly clarifying in their website the answer to the question "Why Learn to Code?: "In a world where we're surrounded by technology and where so many of our interactions we have are with computers, learning to code helps us understand how these services work. What's more learning to code gives us a powerful way to explore our ideas and make things, both for work and play." [14]

---

[8] http://makezine.com/2006/12/01/the-makers-bill-of-rights/ (Accessed 7 August 2014)
[9] http://makezine.com/2014/05/19/adam-savages-10-commandments-of-making/?utm_content=buffer0692b&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer (Accessed 7 August 2014)
[10] Deloitte Center for the Edge (2014), "A movement in the making", http://dupress.com/articles/a-movement-in-the-making/ (Accessed 7 August 2014)
[11] http://www.whitehouse.gov/the-press-office/remarks-president-education-innovate-campaign (Accessed 7 August 2014)
[12] http://www.whitehouse.gov/the-press-office/2014/06/17/presidential-proclamation-national-day-making-2014 (Accessed 7 August 2014)
[13] http://www.tedxbrussels.eu/neelie-kroes/#.U-OOqWPIKcI (Accessed 7 August 2014)
[14] http://codeweek.eu/ (Accessed 7 August 2014)

Supported by easier and cheaper access to tools and expanding communities, the promises and challenges of DIY and making approaches are pointing, in certain cases, towards the ideas of empowering users and democratizing the production of things, thus shifting the control over technology. On one hand, empowerment can arise simply from the act of creation itself, that is, of altering the world around us through a material engagement, following the notion that "our existence is technologically textured, not only with respect to the large dramatic and critical issues which arise in a high technological civilization - such as the threat of nuclear war or the worry over global pollution, with its possibly irreversible effects – but also with respect to the rhythms and spaces of daily life" (Ihde 1990: 1). Making something entails a different type of mediation with your surroundings, potentially a more sensorial awareness of things (Borgmann 1987) or even a sense of craftsmanship (Sennett 2009).

Citizen empowerment through DIY and making also relates to concrete and practical possibilities to embed values, norms and expectations in artifacts themselves, and thus more integrated in particular realities and contexts. Access to technical and communication means to design, modify and create an artifact (object, system, application, etc.) allows for a greater variety of options and choices to be made regarding the purposes, impacts and uses of the artifacts in question, regarding for instance personal health issues, pollution in your neighborhood, or information about local political decisions. In some cases, it is possible to refer to DIY as 'critical making' (Ratto and Boler 2014) when citizens are able to reflect on and intervene in spheres of authority and power through their acts of technological creation.

In this particular sense, through their own technological creations, citizens can enact their understandings of ethical, political, social and cultural issues in ways that are closer to their interests, contexts and goals. By directly engaging in the acts of creating artifacts, citizens are at the same time embedding their values and expectations in artifacts, and regaining degrees of power and control over technology itself. The search of new forms of technological action (Eglash et al 2004) is visible presently for example in movements for transparency, privacy and freedom in information (as in free software and open data), or also in projects for economic justice, human rights, political accountability and sustainability (as in projects like TheyWorkForYou or Open Source Beehives). As such, the most relevant aspect of DIY and making approaches is not a focus on individual capacities and choice for creating new artifacts, but a renewed acknowledgement of questions such as education, power, development, equality or gender, in each citizen's life and in his potential disruptions in material and online worlds.

Rights in-design

The need to balance openness, free flow of information, and protection of individual rights, especially privacy, has led to a variety of tools providing "by design" normativity.

A variety of technological measures have been proposed and/or already implemented to automatically protect individual rights and security, with the aim of doing so more effectively.

Such "by-design" normativity consists of mechanisms "embedded within the entire life cycle of the technology, from the very early design stage, right through to their ultimate deployment, use and ultimate disposal" (EDPS 2010). The European Data Protection Supervisor (EDPS) has strongly supported the by-design approach, referring to it both in normative and technical terms. Privacy by Design has been defined as a "general, binding principle" that has to be included into the data protection legal framework; and also as a technical architecture and design incorporated "in particular ICT areas."
Therefore, the "by-design" approach can be understood not just as a set of technical solutions, but as a specific normative orientation and regulatory principle: namely, the principle of providing default protection to ICT users/citizens. Moreover, and specifically in the domain of surveillance technologies, the Article 29 Working Party asked for Privacy by Design to be made compulsory, "where public authorities are the main actors and where measures increasing surveillance directly impact on the fundamental rights to privacy and data protection" (Art.29 WP 2009).
However, if by-design forms of protection are effective, in technologies for citizens' veillance there is a need to increase knowledge and attention about how technology and normativity co-generate each other, and to open up co-produced loops to transform them into sites for transparent deliberations.

In listing the essentials for an "Internet compact," in 2011 Commissioner Kroes recalled that "architecture matters," referring to how the Internet structures do not only have ethical and policy impacts, but are based on certain values and choices. Therefore, she added, in discussing the "future Internet" there is the need "to have a broad, structured and coherent debate, with the Internet policy and research communities, on the impact of architectural change."

We tend to think of ethical and legal norms as intentional decisions we make about how to act. However, ICT involve also a different kind of ruling as they embody rules and decisions in their own designs and structures. Therefore, if normative decisions are pervading the design of all ICT, the need for open and thorough discussion becomes a matter of democratic legitimacy and citizens' rights.

The widespread modern "prejudice" about the separation between facts and values has been, amongst other things, a major intellectual obstacle to timely recognition and intervention on the values embedded in ICT. The idea that machines and programs can embody values is not new. Already in 1980, in "Do Artifacts have Politics?" Langdon Winner noticed that all machines, structures and technical systems should not only be

analyzed from the perspective of their efficiency and productivity, but also "for the ways in which they can embody specific forms of power and authority" (Winner 1980). These early observations (that have led to a number of developments in ICT, e.g. to make them more "human-centered"), have raised awareness about the choices implicitly embedded, packed, and black-boxed in programs and devices. As Winner has pointed out, "a great latitude of choice exists when a particular instrument, system, or technique is introduced. Because choices tend to become strongly fixed in material equipment...the same careful attention one would give to the rules, roles, and relationships of politics must also be given to such things…"

Now, these normative decisions should be made explicit, transparent, discussed, and controllable, from designers and engineers, to institutions, and citizens.
Rights "in-design" have to be distinguished from "by-design" protection of rights, even though they can be seen as complementary in their pointing at the final product (by-design) and at the process (in-design) (Pereira and Tallacchini 2014). Indeed, the concept of rights-in-design effectively allows extending, deepening, and strengthening the by-design paradigm. If the "by-design" approach aims to create built-in algorithms for law enforcement and rights protection without involving the rights holders, the "in-design" approach aims to raise awareness about the processes through which values and norms become embedded in technological architectures by opening up and making available the choices to individuals as a matter of legal entitlement. [15] If in the "by-design" protection of rights, privacy and data protection are delivered to the user as all-encompassing trusted products (i.e. the process of embedding privacy does not need to be disentangled from the product in order to become accessible); in the "in-design" approach digital architectures and their design are seen as the place where the citizen/user can properly exert their rights and make their own choices about privacy and data.

This also implies a deeper understanding of privacy as a "right" rather than a value covered by legal protection; and highlights that an active role should be recognized to the right-holder, who has to be seen as the real subject of his/her right rather than the merely passive recipient of protective tools designed and controlled elsewhere by other subjects.

Rights-in-design are relevant in several domains, especially when institutions and citizens interact, covering a variety of dimension, from how information is delivered to how laws are implemented.

[15] The European Group for Ethics in Science and New Technologies (EGE) to the European Commission made use of the concept by defining Privacy in Design (as distinct from Privacy by Design) as the process of "raising awareness about the processes through which values and norms become embedded in technological architecture. Privacy in design looks at the normativity of structural choices in an effort to promote transparency and protect rights and values of the citizens" (EGE 2014, 32).

This situation calls for a variety of normative and educational measures to be adopted. Engineers and information systems engineers should work together with ethicists and lawyers in order to build collective transdisciplinary knowledge of the relationships between technology and normativity. Normativity that is consciously and unconsciously inscribed in, and embodied by, artefacts should be made as explicit and transparent as possible before and during the design phase, a crucial stage in development when normative decisions are taken and transformed into programs and functions. Moreover, these normative decisions should reflect and be consistent with the same fundamental values and rights informing legal systems.

2.3.2 A proactive approach to protecting rights: the case for environment and health

Contemporary critical studies in security and surveillance (CSS), especially in the European area, [16] have deeply scrutinized practices of watching and controlling citizens and limiting their rights in the name of their own security, highlighting the potential for abuses (CASE 2006). CSS have proposed a vision primarily centered on human beings and their fundamental rights as individuals, and have suggested replacing the state-centered understanding of security with a project that would have human emancipation as its central concern. From this perspective the connection "security–power–normality is replaced by security–emancipation–normativity, with emancipation disentangling security from power and achieving a fuller and more inclusive realization of security" (CASE 2006, 456).

This "humanistic turn" of the assumptions lying behind security and surveillance has been endorsed by international organizations. After the UN launched in 1994 (UNDP 1994) and re-proposed in 2012 [17] the concept of "human security," namely that security should focus on making human beings, and not sovereign States, more secure, security issues have been increasingly centered on individuals' and communities' well-being as criteria for legitimization.

The centrality of human beings and their rights is strongly informing the overall European ethical and legal vision, and is declared to be at the core of the European policies in the field of cyber- and ICT-security. In the EU vision, security (including cyber- and ICT security) is grounded, to be legitimate, in the European fundamental rights and values as laid down in the EU Charter of Fundamental Rights (Kroes 2013). All activities should respect "the privacy of individuals and their fundamental right to protection of personal data."[18]

---

[16] Leading to the emergence of distinctive European research agenda(s) in the traditionally US-dominated field of 'security studies.' For a comprehensive analysis of the developments of the security field see CASE 2006.

[17] UN General Assembly, Follow-up to Paragraph 143 on human security of the 2005 World Summit Outcome, 25 October 2012.

[18] Communication from the Commission to the European Parliament and the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM(2010) 673 final, Brussels, 22.11.2010.

This rights-based and fundamental—and even constitutional—values-oriented approach is even more necessary in the quest for legitimacy and good practices when surveillance technologies are used by private citizens in performing their activities. The existence of these conditions, namely respect for fundamental rights and the protection of constitutionally agreed values is proposed here as the threshold for considering the legitimacy of these activities for defining the boundary between sur-veillance, sous-veillance and veillance.

This is why, in exploring and assessing different experiences and case-studies, the interconnected fields of health and the environment—and environmental health—appear as the most prima facie socially, ethically, and legally promising applications. Indeed, health and environment are amongst the most frequent domains for citizens to engage in veillance activities. Two broad categories can be envisaged. One consists of those forms of self-surveillance for self-help purposes directed to protect surveillants from specific risks, and possibly to prevent them from harm (with or without external assistance from a third party). Historically, these initiatives have often concerned patients with chronic diseases. People are empowered by becoming experts in managing their own disease, through the use of ICT sensors and by communicating and sharing data and experiences in dedicated social networks.[19] Collective and shared self-surveillance thus contributes to empowering patients-citizens in several ways: by enhancing their knowledge of the disease and raises awareness of their own situations; by increasing independence both from doctors and from family; and, by extending their freedom and mobility while maintaining safety through discrete accepted control. Efforts by communities to monitor industry's effects on air quality have been another kind of widely performed participatory surveillance. Communities have used a variety of strategies and devices to watch and control the environmental impacts of neighboring industrial facilities to establish connections between levels of pollution and the emergence of specific diseases (Ottinger 2010). These activities have been mostly named and interpreted as sous-veillance, even when some of them lack the symmetric surveillant gaze, namely community members being watched by industry. In the connection between environmental conditions and privately-performed participatory surveillance, the seemingly separated domains of health and political powers in democratic societies merge. The forms and the subjects of knowledge production-and-use involved in these activities aim to co-produce knowledge as a form of power.

While environmental monitoring is performed to protect public health, this form of surveillance has become a strategy for the political empowerment of a community. "In

[19] See, e.g., an initiative defined as "participatory surveillance" and led by the online organization Tudiabetes.org (http://www.tudiabetes.org/), allows diabetic insulin-dependent individuals to prevent hypoglycemia episodes through continuous monitoring of their blood sugar and through constant control within a social network (Weizman et al. 2013).

its contemporary form, surveillance is undertaken with an eye to intervention. That is, surveillance is not simply the act of watching, of collecting numbers, images, and other data to track activity. A second, constitutive part of surveillance is the goal of influencing or managing those whose data have been garnered" (Ottinger 2010, 221-222).

In fact, the specific empowerment fostered by environmental and genetic surveillance depends on the meaning of the gathered data. Knowledge generated through direct collaboration between scientists and citizens is both trusted by participants and relevant for authorities (and industry) (Ottinger 2010).

Computational technologies which aggregate data about individuals to create populations that can be acted on are critical in transforming data into interventions; and social networks not only give interested people the ability to connect to each other and with scientists, but also to transform rarefied scientific activities in social movements. Now, unrelated and even isolated citizens from different places are quickly learning how to empower themselves to become aware of, and exert, their rights by transforming knowledge and technology into civil and community life.

3. Theoretical Insights

3.1 Reflecting on Citizens' veillance

As described at the beginning of this report, the workshop aimed to propose a double reflection on citizens' veillance activities, by first focusing on some major theoretical dimensions, and then by looking at practical experiences. The theoretical section looked into three main areas relevant to the topics explored: the meaning(s) of privacy and the need to make sense of them in different contexts; the current approach to surveillance in the context of European ethical perspectives; and the relations between participation and empowerment in surveillance activities.

The three key-note speakers also conveyed perspectives brought from the scholarly and the institutional cultures as well as from the US and the EU environment. Helen Nissenbaum, Professor of Media, Culture and Communication, and Computer Science at New York University (USA), opened the conversation by discussing a fine tuned, context-dependent vision of privacy. Jim Dratwa, Head of the Ethics sector in BEPA (the Bureau of European Policy Advisers to the President of the European Commission) and of the EGE Secretariat, explained their ongoing work of the EC European Group for Ethics in Science and New Technologies on their Opinion 28, dealing with "Ethics of Security and Surveillance Technologies," which was later published on 26 May 2014. Anders Albrechtslund, Associate Professor of Information Studies at Aarhus University in Denmark, analysed the lights and shadows as well as the ambiguities associated with the notion of participatory surveillance.

3.2 Respect for context as a benchmark for privacy: what it is and isn't

Nissenbaum started her presentation illustrating the Privacy Bill of Rights endorsed in February 2012 by the Obama White House. The Bill comprises seven principles. The third, "Respect for Contexts," is explained as the expectation that "companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data." The principle has given rise to heterogeneous and contested interpretations, as parties representing diverse interests attempted to make theirs the authoritative one. Nissenbaum presented three different interpretations and explained none of them allowed going beyond the status quo, which regulators in the US, Europe, and beyond have found problematic. Indeed, the issues of transparency and choice in their translation to current privacy policies (e.g. zappos.com privacy statement) have not been adequately dealt with. In the US, although at first there was a lot of support for the Privacy Bill of Rights in 2012, the advocacy community is now disappointed.

Although the philosopher considered influencing policy as an important goal, her main approach in the talk was more about presenting an underlying justificatory or normative rationale than establishing explicit rules for privacy.

Nissenbaum introduced the concept of "contextual integrity," namely respect for context, arguing that it offers the best way forward for protecting privacy in a world where information increasingly mediates our significant activities and relationships. Contextual integrity is a specific notion that differs from existing approaches, and is in harmony with basic intuition about information sharing practices and norms (Nissenbaum 2009).

Nissenbaum has been working with computer scientists to define and establish "context-specific informational norms" to be applied to systems. The concept of "contextual integrity" that she has developed offers the possibility to focus on context-specific purposes and values. For example, in healthcare, context relates to curing diseases, alleviating suffering, providing equity.

The concept can be seen as brutally ambiguous in its complete dependence on the meanings that are assigned to it at the discretion of the reader: for technology designers context can refer to a technical system/platform, for industry representatives it can be defined as a particular business model the consumer is interacting with, or, otherwise, it can be seen as the social context.

Despite these ambiguities, it can be borne in mind that the right to privacy is neither the right to control information nor the right to secrecy. It is more about the "appropriate flow" of information in society. Sharing information is a social good, and therefore secrecy has to be restrained to particular situations.

Still, it is not completely clear which "information principles" (e.g. control, consent, coercion, buying, selling, confidentiality, etc…) should hold, and which "transmission principles" should define information flows that respect contextual privacy.
Moreover, we have to be aware of the presence of "disruptive flows:" for instance, publishing something on the Internet can introduce a disruption in the information principle. The evaluation of disruption/disruptive changes often depends on conflicting interests, and general moral, social and philosophical rights and values. Privacy expectations, for instance, may change in relation to what each technology can do (e.g. facial recognition in Facebook). Moreover, technological affordance should be separated from moral values. Social contexts impose substantive constraints, which in turn can generate rules based on e-norms, shaped by ends, purposes and values. Algorithms for obfuscation such as TrackMeNot and Context Aware Do-Not-Track can help in this respect offering protection to users.

During the discussion following Nissenbaum's presentation, participants highlighted the interest but also the problematic issues raised by contextual privacy, especially the implications of reducing the complexity of human interactions to separate contexts, and the difficulties of dealing with overlapping and mixed contexts.

3.3 Reframing security and surveillance technologies: ethical experimentations of Europe

The European Group for Ethics in Science and New Technologies started dealing with ICT only in 2012, when they were asked by EC President Barroso to explore the ethical implication of information and communication technologies (Opinion 26, EGE 2012). In 2013 President Barroso asked the EGE to continue their analysis in the field by taking a close look at the "Ethics of Security and Surveillance Technologies." Shortly thereafter, the Snowden case revamped the issue of surveillance technologies all over the world. When the Workshop took place in March 2014, however, Opinion 28 was still in progress (later released on 26 May 2014.

As a consequence, while Jim Dratwa's speech could not illustrate the EGE's specific conclusions and recommendations, it highlighted some major questions that the Group was dealing with as well as the main features of a European approach to security and surveillance.

What do we want to secure? Why and how, and at what price? What do we want to make or keep safe? And who is the 'we'? But also: are we sure that our tracking technologies are so powerful, when a case such as the disappeared Malaysian Boeing 747 in March 2014 seems to show blind spot in the global Panopticon?
Contending narratives and imaginaries exist with regard to the ethics of security and surveillance technologies—and their attendant practices and institutional arrangements—that need to be traced and scrutinized. These narratives mobilize and probe the prevalent articulations of knowledge and action, as well as the modes of production and validation of knowledge and values.

The prevailing narrative set forth to argue for different ways of framing and balancing issues of security and surveillance are the following: the trade-offs between security and freedom, namely the assumption that in the name of security people should accept to give up some of their liberty rights; the balancing perspective, where rights cannot be suspended, but carefully defined in each context in relation to security; the "blind spot" and the "light spot" discourses, highlighting that we don't know where, how, and by whom decisions are made. In this respect, many blind spots exist in what we believe to see as transparent. For example, the legitimate defence vision, which arguing for the necessity of security and surveillance measures to protect citizens, or the quarantine narratives, which justify the infringement of individual rights (quarantining infectious individuals) in the name of a public good (protection of public health) when the risk was created by a specific technological innovation policy, such as xenotransplantation experimentation, the use of cells and tissues from swine to humans.

Therefore, on the backdrop of evolving forms of open science, citizen science, big data science, the actual possibilities given to—and opened by—citizens to be empowered need to be analysed and questioned.

3.4 Participatory surveillance and citizens' empowerment

The topic and the issues of participatory surveillance were introduced by Anders Albrechtslund, whose research has mostly focused on surveillance, social media, and ethics. Albrechtslund highlighted how, in later years, a number of scholars have proposed ways of understanding surveillance that challenge dominant perspectives such as organizations, power relations as well as negative, Big Brother-inspired, emotions. This direction of "post-Panoptic" approaches, as they might be described, includes the study of the experiences of the subjectivity engaged in surveillance practices, e.g. as resistance, empowering exhibitionism or participatory surveillance.
According to Albrechtslund, it is very important to further explore these forms of citizens' empowerment, and thus to continue this trajectory of thinking. His intention is to introduce an understanding of surveillance that makes room for practices that support, expand, and facilitate everyday activities and social interactions such as peer- or self-surveillance.

Even though surveillance can be never seen as neutral, it does not make sense to characterize it as 'good' or 'bad' in broader terms. The actual quality of surveillance depends on specific contexts and personal experiences. Therefore, a pluralistic approach to surveillance is needed that can include different concepts of surveillance while contrasting all absolute, exclusive definitions. This is a new direction in the study of surveillance and social media, that makes it possible to elaborate our understanding of both. The basic observation is that new media offer spaces where surveillance can be used proactively to facilitate social interaction, entertainment or civic engagement. Rather than being an unpleasant, unwanted and dominating gaze, surveillance here is also a practice that people actively engage in for purposes ranging from empowerment to playfulness. By deciding to share selected information about themselves, people may be willing to participate in their own surveillance as part of everyday social life.

4. Practical Insights

4.1 Citizens' veillance in practice

The second part of the workshop reflected upon citizens' veillance through the lens of various experiences related to several areas of social concern and the protection of public goods. Practical insights were taken from a variety of fields grouped around three main domains; research groups; health, environment, and human bodies; and artistic activities involving civic science. The first session included presentations on citizens' veillance techniques as experienced by two research groups, namely the UCL ExCiteS research group (Michalis Vitos), which uses ICT to empower indigenous communities in Africa in protecting biodiversity, and the JRC research group on participatory surveillance (Fivos Andritsos), which explores the implications of surveillance technologies for collaborations between citizens and public authorities.

In the second session of citizens' veillance in practice, three sectors were identified as particularly well suited for understanding and assessing practical applications of the concept; environment, health, and the human body. The projects and speaker in this second session were selected to illustrate citizens' veillance in these sectors. Each project is characterized by the merging of academic and scientific knowledge along with more experiential, self-taught and DIY knowledge. The project teams were often comprised of traditionally defined experts (such as medical professionals and computer programmers) along with communities and public groups with less experience in knowledge generation projects. In the first presentation Annibale Biggeri, epidemiologist and engaged scientist from the University of Florence (Italy), described several case studies of citizens' empowerment through genetics and ICT. This was followed by Willis Elkins, representing the civic association Newtown Creek Alliance (USA), who described his own photographic contribution and commitment to help other citizens in surveying—and hopefully reviving—polluted suburban areas of New York City. Finally, Adriana Lukas, the leader of the UK Quantified Self (QS) group, described the new unfolding practices of quantifying several bodily aspects and functions that are at the core of the Quantified Self movement—the use of wearable sensors and other ICT to explore numerical translations of ourselves. Lukas explained the theoretical stances and increasingly numerous applications that are not only reframing the individual and social perception of the body, but are also creating opportunities for citizens' empowerment.

In the third session, speakers discussed their experiences of the use of ICT for artistic civic science. Mónica Mendes (University of Lisbon and M-ITI, Portugal) and Pedro Ângelo (void.io, Portugal) embedded the workshop and the participants in the video experience of natural green landscapes to show how artistic video surveillance can contribute to raise and educate people's environmental awareness. The last presentation, by Pablo Rey, from Public Lab and Basurama (Spain), focused upon DIY balloons used to map the territory as a way to help community building.

The overall impression created by the wide variety of citizens' veillance projects, of the values embedded in them as well as in their technical means, of the concrete practices and the existential experiences they were conveying, offered the most insightful evidence of the goal of the workshop: how ICT in citizens' veillance are deeply modifying our sense of knowledge and social life.

4.2 Research Group 1 - Taking Citizen Science to Extremes: From the Arctic to the Rainforest

Citizen Science is hardly a new concept. In fact, it is present in many past initiatives and in current projects around the notion of participatory sensing. In particular, Muki Haklay has proposed a framework for the level of engagement of participants in citizen science activities, dividing it in four levels: 1) crowdsourcing (citizens as sensors); 2) distributed intelligence (participants as basic interpreters); 3) participatory science (participation in problem definition and data collection); and 4) extreme citizen science (collaborative science – problem definition, data collection and analysis).

During the last decade the interest for citizen science received renewed attention in both academic and popular interest. This trend is in part driven by an increased interest for open paradigms, as well as Information Communication Technology (ICT) innovations such as smartphones, mobile Internet and cloud computing. This has given rise to the emergence of a growing and highly diverse crop of new—and often innovative—initiatives.

Whilst there are often significant differences amongst projects, for instance when it comes to power relations—"Who is working for who?"—or the determination of goals and outcomes—"Who is solving whose problems?"—there is hope that, at the very least, this rediscovery of citizen science might lead to a renewed mutual interest, and perhaps understanding, between scientists and the general public. Most citizen science initiatives are set in affluent areas of the world, and by and large they target an educated, or at least literate, public.

Extreme Citizen Science (ExCiteS) aspires to extend the reach and potential of citizen science beyond this restricted context, and is defined as *a situated, bottom-up practice that takes into account local needs, practices and culture and works with broad networks of people to design and build new devices and knowledge creation processes that can transform the world*.

ExCiteS has launched several projects, such as Mapping for Change, Citizen Science Games, and other initiatives. All these initiatives (and the tools involved) were co-designed with users.

The projects span from the Arctic—where we aim to develop tools grounded in the needs of Yupik and Iñupiaq coastal subsistence hunters, who are adapting to the rapidly changing climate—; to the Congo basin rainforest—where we enable marginalised and forest communities to better and more effectively share their vast environmental knowledge locally and with other regional, national, and global stakeholders. ExCiteS aims to design, develop, evaluate and deploy a generic platform that enables people with no or limited literacy—in the strict and broader technological sense—to use smartphones and tablets to collect, share, and analyse (spatial) data along with a methodology for introducing, engaging and empowering marginalised communities to participate in, and benefit from, citizen science. The platform is and will be used in a variety of concrete projects, often related to environmental monitoring. Ultimately the goal is to let communities build so-called Community Memories: evolving, shared representations of the state of their environment, their relationship with it, and any threats it faces.

Michalis Vitos, from the ExCiteS group, focused his presentation on a specific project - participatory monitoring in Republic of Congo. The overall process consists of an iterative and participatory software development, where the researchers implement free and informed consent, and built community protocols about the project, the stakeholders, and the use of data. Indeed, the process itself is very important as the community has to decide what is important to collect. Data are then incorporated in the software programme, thus modifying the type of data to be collected. Therefore, members of the community enter the forest and map what they want to highlight. This is a clear example of feeding data back into communities and a new way of visualizing the data.

From the start the main challenges and limitations were illiteracy, lack of electricity, and lack of networks. The solutions provided by the group encompassed using robust Android touch-screen devices, and Sapelli data collectors (pictorial icons for selection, audio, video). To solve the problem of connectivity, participants sent information by SMS to a mobile phone which was situated in a NGO office. The phone, which had access to the internet, could send the data on via an Amazon server.

Other limitations experienced in the project have been related, for instance, situations where participants wanted to map their tools, or create a community application. Unfortunately, these activities were not possible because the project was limited to mapping resources. Further development would require more training and guidance.

4.3 Research Group 2 - Future Surveillance: The Citizen in the Loop or in the Loupe?

A group of researchers at the JRC is exploring different ambiguous aspects of participatory surveillance. In fact, modern ICT offer formidable opportunities to citizens and society, but also pose severe threats to our privacy and civil liberties. Although our

perception of such opportunities or risks depends on our values and priorities, it is extremely dynamic and context-sensitive. Ideally, the various security tools and methods must also be context-sensitive, adapting to the priorities of society or societal groups; in particular, when security tools require the active participation of citizens. Fivos Andritsos's presentation outlined a citizen-centred model of perceived risks and threats, analysing current trends in surveillance technologies and the performance of current centralized hierarchical emergency management systems.

Two cases of novel, context aware ad-hoc networked surveillance systems were illustrated. These systems are designed to capture and transmit information only upon the occurrence of certain events that, beyond any reasonable doubt, constitute severe threats. Such systems are based on the use of autonomous, sensor-based "agents" that react to changes in their environment, collecting and dispatching useful information only when and where required. For instance, the right of not being observed can be implemented for instance in static obfuscation of parts of the screen, or dynamic obfuscation of objects. In the JRC, research was conducted as proof of concept by separating images (sensitive data such as face and body) through IR-based low cost 3D cameras.

The first system allows the prompt location of persons trapped under the ruins of collapsed buildings (LOCCATEC), while the other serves for emergencies in the public transport domain (ASPIS). Referring to these systems, Andritsos argued for a novel concept of "participatory situational awareness" in case of emergencies that is based on the active participation of smartphone equipped citizens. The idea is to actively involve the smart-phone equipped citizens as nodes of an ad-hoc sensor network that will provide, in an organized way, near real time information to manage the emergency. The proposed system would empower citizens to use their smart phones not only to send an alarm or to receive notifications, but also to provide useful information to the emergency centres in a coordinated way.

Andritsos argued that, as the values connected to privacy change according to contexts (you don't want to have cameras in your room when you sleep, but in an earthquake you wish that a camera will be able to find you), context aware surveillance is important.

Finally, the presentation focused on the potential advantages, but also drawbacks and issues regarding the bottom-up approach proposed by the citizens' veillance principle. Some of the main issues and risks are: conditions giving rise to location request; how fast you are able to locate smartphones (15 minutes now, but you can do at seconds in systemic level); and mutual trust between authorities and citizens. The issue remains: how can citizens enter the loop through bidirectional capacity and in a reciprocal way?

4.4 Health - ICT and Genetics to Empower Citizens' Health

Turning to the domain of health, Annibale Biggeri focused on how, in the last decade, three different phenomena have merged: the widespread use of ICT devices to collect and potentially share personal and scientific data, and to build networked communities; biobanking for genomics, namely the organized storage of human biological samples and information; and the collaboration between scientists and citizens in creating knowledge, namely peer-production of knowledge for shared social goals. These different forms of knowledge, technical tools, and skills have merged in community-based scientific and social, as well as legal initiatives, where scientists-and-citizens use genetic information and ICT as powerful means of gaining more control over their health and the environment. These activities can no longer be simply qualified as epidemiological research and surveillance. Instead, they can be framed as new forms of citizens' participatory veillance, an attitude of cognitive proactive alertness towards the protection of common goods. The initiatives illustrated by Biggeri, where he is acting as an academic and an engaged scientist directly helping the population, concern two Italian groups of citizens and scientists who are making use of both ICT and biobanking to protect environmental health in highly polluted contexts. One initiative is named "Fondazione Bioteca Sarroch" (Cagliari, Italy), from the city of Sarroch, near an oil refinery plant; the other is the project "PM2.5 Firenze," for the control of particulate matter in the city of Florence. In both situations, citizens—scientists and lay-experts—started a knowledge-based activity to re-establish some fundamental rights, after these have been infringed (or are at risk of being infringed), by "privately" producing valid and more transparent knowledge, and to complement or even confront official, institutional knowledge. In both cases, aimed at minimizing public health impacts, the theoretical framework included the precautionary principle, uncertainty analysis, and extended democratic debate, merged with ICT and genetics, to empower people.

In the Sarroch Bioteca Foundation experience, the Sarroch municipality, together with other stakeholders, promoted the project in 2006 as a complex set of epidemiological investigations with the purpose of using science for timely policy measures. All phases of project were discussed and agreed with the local community as a form co-production of knowledge. Often Biggeri used the first person plural "us" to refer to himself and to the other citizens, highlighting his experience of "undivided self," acting as a scientist and as a civic stakeholder.

The biobank was planned to be physically located in the village, and the foundation was set up as an independent entity collectively owned by citizens—rather than being hosted within a scientific institution. The Sarroch Bioteca Foundation was officially recognized on August 2012, and is established as a trusted entity. All citizens are entitled to be members, but they are asked to formally give their adhesion to the project, and subsequently to freely volunteer (through an ad hoc informed consent) to be enrolled in specific research by providing their biological samples.

The Bioteca is an example of citizens' veillance as the initiative came from the community/municipality and not by institutional bodies (which could lead to lack of trust and conflict of interests) and because there was no direct watching on the industry, but only to genetic changes as indicators of health.

As to the PM2.5 Firenze case-study, this is a project of citizen autonomous monitoring performed with private tools in Firenze, where citizens do not trust the institutional data about environmental pollution from particulate matter.

During the following discussion, a question was made about the potential mismatches between the goals of the researchers and the population. Biggeri raised the issue of the mismatch of the different times and processes required by engaged and academic science, or more properly by science for policy measures and for publication in peer-reviewed journals. A different question concerned the community actual engagement and citizens' control over the process in Sarroch. Biggeri observed that the Foundation is a trusted entity with a board of directors, where all decisions require people's consent and the biobank belongs to the community.

4.5 Environment - Citizen Surveying within Polluted Areas

Willis Elkins shared with the workshop participants his experience and initiative in advancing, together with other citizens, the revitalization of New York City's urban waterways and their surrounding environs. Elkins's direct explorations and interests in larger collaborative-based projects have given way to a series of initiatives that have helped increase public knowledge and awareness about water and air quality issues.

A number of citizen driven surveys are beginning to answer some of the long-standing questions about environmental and human health issues. In all instances, such citizen survey projects arose in response to the data collecting and sharing standards employed by the governmental agencies responsible for environmental monitoring and public health hazards. It is their goal that with low cost technologies, creative approaches, and volunteer efforts such projects can demonstrate new models of surveillance and data collection that will supplement and even advance the future efforts of the responsible agencies.

Newtown Creek is one of the most overlooked and significantly polluted urban water-bodies in the United States. The Newtown Creek Alliance is centered on an 11 mile creek which was once the busiest industrial canal in the region, also gathering domestic and farm waste. As the area has few access points, Elkins bought a small boat and primarily focused on visible, floating debris/waste. Having suffered two centuries worth of industrial use and abuse, this once ecologically rich salt marsh now stands as an underutilized and relatively inaccessible canal in the geographic center of New York City. Despite improvements in pollution regulations the landscape of various

environmental harms is exceedingly vast and complicated, notably: widespread chemical and heavy metal concentrations in soil and sediment, remediation of the 2nd largest oil spill in US history, ongoing untreated sewage discharges and street runoff, chemical plumes under residential areas and excessive truck traffic from the surrounding network of waste transfer stations. The various governmental involvement and cleanup oversight (city, state and federal) have created a separate complicated tapestry of data-collection, communication, responsibility and enforcement. In this context, do-it-yourself surveying has allowed concerned citizens and organizations to better expose and understand a number of issues and conditions that may otherwise be hidden, dormant or simply poorly documented.

Four citizen driven survey projects, where Elkins has been involved, were discussed as especially relevant:

1. A harbor-wide water quality testing program that focuses on locations where users are most likely to come into contact with potentially bacteria filled water, i.e. the edge of a dock or shore. The project collected water samples, showed data online, and also produced painted murals with different colors indicating the safety and quality of water for swimming.
2. A weather station network setup to determine local rainfall in a single watershed. Information is correlated with sewer overflow levels and alerts citizens (via SMS and Twitter) to such events.
3. AirCasting - a platform for recording, mapping and sharing air quality data metrics, such as CO and particulate matter, via a smartphone and low cost sensors. Sessions are displayed in real time and added to a shared online map.
4. On-going low tech surveying of various species of wildlife that have returned to Newtown Creek in recent years. Exploring difficult to access areas we use surveys and photographs to tell the encouraging story of life living in a Superfund site.

During the discussions, Elkins explained that a large portion of the crowdsourced funding is spent on software development, although these ICT tools are then released with open source licenses and, therefore, can be reused for other settings.

4.6 Human body - The Self in Quantified Self: A Perspective on Personal Data Autonomy

Adriana Lukas, founder of the UK section of Quantified Self (QS), explained the philosophy and practices of this rising phenomenon of self-tracking, briefly defined as measuring aspects of one's life. Lukas has been organizing Quantified Self meetings since 2010. The potential for quantifying personal life, combined with ubiquity of personal data, has attracted interesting reactions from institutions, businesses, and the media.

Within the movement, there are currently two competing tracks: 1) supply side (Fitbit, etc.), with technologies designed for and marketed to the general consumer, and 2)

demand side, where people want to solve a problem, for instance how to measure certain aspects of their life, how to make sense of the data, and how to use all that to improve their lives.

The creation of a new class of personal data, more personal than ever, has brought urgency to citizens' privacy and data ownership. It has also opened up new potential for meaningful uses of data by individuals and for data literacy. However, without certain technological underpinnings, specifically a form of personal data infrastructure, there is danger that QS will be another data source for aggregate data analysis, which threatens to diminish citizens' autonomy over their personal data.

In the context of the workshop, the main question concerns the actual citizen's empowerment through QS methods. Is the current user data model created around platforms capable of evolving to provide sufficient control to individuals over their QS data? There is a growing tension between Open Data and Personal Data as the benefits of the former become obvious and personal data becomes an attractive resource for common good analysis.

From the technical point of view, Lukas mentioned the issue of databases in terms of its acquisition, data storage (in a secure way and access), and data analysis (mining and visualization). At present, all applications perform all these three aspects, but in an unsatisfactory way; and the result is fragmented personal data locked in different sites. There are open source alternatives, where users can store data in their own server if they are skilled enough (e.g., Angelsensor.com or Fluxtream.org). Therefore, a current major issue regards open formats and exportable data. The possible solutions to store data are the following: a database on an owned server, a database on a third party platform, or a database on a personal cloud server. In Lukas's view, for self-analysis to be useful, it is the individual who has to pose the question and make the decision. Another issue concerns machine learning, namely that, in order to really empower citizens, powerful analytical tools are necessary. In the end, what is needed for further developments is a "personal data infrastructure."

In the following discussion, the issue of individual empowerment in Quantified Self was raised: do non-experts have the capacity to collect and interpret data by themselves? Are these systems intelligible to average citizens, or are they becoming increasingly complex? Concern was expressed over the present distance between these systems and users when complex processes or criteria predefined by experts are involved. Adriana Lukas recognized that the Quantified Self community is still a relatively small and specialist community, that is highly motivated and skilled; however, over time, systems will get simpler and easier to be used by a wider range of citizens.

4.7 Art & Civic Science 1- Appropriating video surveillance for art and environmental awareness: experiences from the ARTiVIS Project

Artists and researchers Mónica Mendes and Pedro Ângelo presented the history of the ARTiVIS project, described ongoing research work, and shared their views on how surveillance technology can be appropriated for artistic, educational and civic engagement purposes. Invented and led by them, the ARTiVIS (Arts, Real-Time Video and Interactivity for Sustainability) is a research project that explores how real-time video can be used as a tool for environmental awareness, activism and artistic explorations.

Through a collaborative approach involving artists, technologists and activists, the project seeks to develop digital contexts for aesthetic contemplation of nature, fostering environmental awareness and empowering local populations through DIY surveillance. At the heart of the project are the interactive art experiences B-Wind!, Hug@ree and Play With Fire that use real-time video as raw material to promote environmental awareness through the "emotion of real-time". The project focuses on the user's experience through positive feedback in a local context.

Mendes and Ângelo underlined the importance of community workshops, namely to teach people how to assemble these kits and to customize them for their own purposes. The artists are also interested in "community-driven sensor networks," where users own the data and can use them for public purposes. Through the DIY forest surveillance kit, for instance, communities are enabled to protect their own forests through an online peer-to-peer forest surveillance network based on an affordable DIY forest surveillance hardware kit.

The technical challenges involved by these activities are still mostly represented by security problems of IoT platforms, while on the social side accessibility and sustainability are the major issues. Looking ahead, some of the expected developments will include telepresence, cyberphysical systems (single platform and make them accessible to people), and blockchains (trusted peer-to-peer database).
During the following discussion, the issue of low profit was raised as these activities can be hardly thought as path towards better sustainability or broader models for social innovation. The case of "Goteo",[20] in Spain, was mentioned as a form of crowdsourced platform not only related to money, but also to other resources, such as the provision of code for delivering computer programs.

[20] See at http://goteo.org/about (Accessed 21 August 2014): "Goteo is a social network for crowdfunding and distributed collaboration (services, infrastructures, microtasks and other resources) for encouraging the independent development of creative and innovative initiatives that contribute to the common good, free knowledge, and open code. We support projects with social, cultural, scientific, educational, technological, or ecological objectives that generate new opportunities for the improvement of society and the enrichment of community goods and resources."

4.7 Art & Civic Science 2 - DIY balloon mapping workshops in Spain. Documenting the territory and community building

"Defiende el territorio desde el aire" (Castellón, Spain) is a project developed by Pablo Rey Mazón and the organization Basurama that aims to start a local chapter of balloon and kite mappers in Spain, using Public Lab tools. A workshop was organized with citizens in Castellón with the aims of showing the basics of low cost balloon mapping techniques to document the territory; starting a small community of users; and, finally, awaking the inactive Spanish language Public Lab mailing list.

Public Lab is an open community of users and citizen scientists who investigate environmental concerns using inexpensive DIY techniques. Low cost, DIY tools can allow a wide range of users (activists, photographers or mappers) to document and experiment with their own data. In order to help people become more aware about their own struggles, Basurama made a public call and contacted different local environmental groups and citizens in the region to organize a 3 day hands-on workshops (January 31st – February 2nd 2014). The groups were asked which places they would be interested to map and they collaboratively wrote a list with potential locations. Basurama wanted to support ongoing local environmental struggles that were already taking place for the defence of the territory. To extend the reach of the workshop one balloon mapping kit with a camera and a bottle rig was made available to the workshop participants during the 3 months that the exhibition lasted, until April 27th 2014. All the information produced was licensed under free licenses and is available online. The workshop was produced thanks to the invitation made to Basurama to participate in an exhibition to continue its documentation project 6000km.org. The results of the workshop—maps and photos—are now being displayed in an art exhibition at the Espai d'art contemporani de Castelló (EACC).

5. Insights from the Discussants' Session

5.1 Discussing Citizens' veillance

Three pre-identified discussants were invited by organizers to start the general discussion by either summarizing some previous themes or highlighting some other aspects related to citizens'' veillance. Anne Wright, engineer and PI of the BodyTrack Project at Carnegie Mellon University in Pittsburgh (USA), Apostolos Malatras, information systems engineer and researcher at the JRC (Ispra, Italy), and Stéphane Chaudron, pedagogist and researcher at the JRC (Ispra, Italy) contributed their distinct perspectives to the overall debate.

5.2 Self-tracking: Reflections from the BodyTrack project

Anne Wright continued and deepened the reflection on ICT for surveillance and the human body in the perspective of self-tracking. Self-tracking has been shown to have the potential to empower individuals to explore and address issues in their lives and share their experiences in building tools and fostering culture to support people to learn and engage in such practices. Anne Wright's research has been inspired by examples of people who have reclaimed their wellness through iteratively noticing patterns of ups and downs, trying out new ideas and strategies, and observing the results. In some cases, individuals have realized that certain foods, environmental exposures, or practices have unexpected effects for them, and that adopting custom strategies can greatly improve quality of life, overcoming chronic problems in areas such as sleep, pain, gastrointestinal function, and energy levels. Importantly, adopting the role of investigator of their own situation appears to be empowering: people who embarked on this path changed their relationship to their health situation even before making discoveries that helped lead to symptom improvement.

Anne Wright's experience and expertise has given rise to the BodyTrack project, which has the goal of empowering a broader set of people to embrace this investigator role in their own lives and better address their health and wellness concerns, particularly those with complex environmental or behavioural components. Wright's research is framed as a participatory design work, in the sense that it is conducted always with users and that is passed from one user to another. The core of the BodyTrack system is an open source web service called Fluxtream (https://fluxtream.org) that allows users to aggregate, visualize, and reflect on data from a myriad of sources on a common timeline. These data sources include physiological metrics from wearable sensors, image and self-observation capture from smart phones, and contextual clues of what was happening when in their lives such as location tracking, calendar entries, notes, etc. The project aims also to develop and propagate peer coaching practices to help transfer the culture and skills of self-tracking while fostering individuals to self-assess and guide the process for themselves.

Other projects are ongoing in the CREATE lab at Carnegie Mellon that are performing forms of citizens' veillance through low cost air and water monitoring.

5.3 Participatory Surveillance project at JRC/IPSC.G07: output and experiences

Apostolos Malatras offered further elements to think about participatory surveillance. Participatory surveillance is a novel research theme that is based on the willingness of citizens to share data collected from the sensors embedded on their smartphones and the utilization of this data for the purpose of providing added value security and surveillance services. A prominent scenario that illustrates the potential of participatory surveillance systems is that of crisis management, since it could provide the teams of rescuers with a wealth of information about the people inside buildings even in the absence of operational networking infrastructures, using merely raw sensor data. The latter yield no significant information as such, but subject to processing using machine learning techniques it can be used to deduce useful knowledge about the activities the users were conducting at the time of data collection.

In the context of the participatory surveillance project conducted by the research team of IPSC.G07, the processing and analysis of sensor datasets collected from emergency scenarios are studied in order to be able to infer human activities from raw sensor data. In particular, based on an emergency evacuation experiment that was conducted at the premises of JRC in January 2012, the JRC team collected sensor data, namely accelerometer, gyroscope, magnetometer values, from the sensors embedded on smartphones carried by the actors of the experiment. Despite the shortcomings of the experimental settings and the limitations in terms of sensors' accuracy that the researchers endured, they were able to capture enough data that allowed to proceeding with the analysis. They introduced a methodological framework of preprocessing relevant data, cleaning them to remove outliers, applying windowing to generate instances and finally applying statistical features extraction techniques on them to acquire a better understanding of the data. Having selected the most appropriate classification algorithms for our scenarios, the team proceeded by applying them on the datasets collected during the evacuation exercise and tried to predict the type of activity that the users were engaged in at the time of data collection.

Despite the shortcomings in the experimental setup that led researchers to use solely accelerometer readings, the selected classifiers perform extremely well with prediction accuracy reaching 99% in some cases, e.g. when considering reference datasets that were collected for testing reasons. Based on the findings the JRC researchers could assert that there is great potential in further work on participatory surveillance, since even with the meagre and low-quality accelerometer data, they were still able to infer users' activities with sufficient accuracy. The group postulates that by using a richer set of collected datasets and applying sensor fusion techniques they may be able to

improve the quality and precision of class predictions and, subject to more detailed reference datasets, the type of class could be pinpointed at a higher granularity.

The analysis of the results, and the possibility of predicting with high accuracy the class of previously unclassified data, has highlighted the great potential of participatory surveillance systems. It has also exposed the great privacy risks regarding users sharing data from their smartphones from such systems. According to Malatras and the other researchers involved in the project, the use of additional sensors and the information fusion emerging from the use of multiple sensors will exacerbate these privacy risks and allow for more accurate prediction of the users' activities, as well as the context of his/her surroundings.

Traditionally users are most hesitant and self-conscious about sharing their location and camera feeds, but one can expect that average users may agree to share their accelerometer or magnetometer data without appreciating the inherent risks involved with such an action. Typical examples of such risks reported in the literature include the possibility to infer the PIN of users on smartphones or the password that they type using accelerometers and gyroscopes, and lately the camera and microphone of a smartphone. The stealth nature of some of these sensors and the implicit assumptions made by the users that these sensors do not expose any of their private data are two causes that necessitate further research in the domain. The expected outcome of such research includes a risk assessment of participatory surveillance sensors and a set of guidelines for the optimal protection of sensitive user data (Data Protection Impact Assessment - DPIA).

5.4 Baby-tracking: When monitoring children becomes tracking children

Stéphane Chaudron introduced the topic of tracking children and critically discussed the risks connected to these emerging practices as some ICT tools are becoming increasingly common. A recent Wi-Fi remote baby monitoring device allows parents connected via smart phones or tablet to first get a wide view of their baby's room, even when dark. thanks to its infrared Night Vision LEDs. They can zoom into the bed and to check in on the baby, to hear its calm breath. The advert claims to allow parents to be '*Always near* their baby' and the baby to be '*never alone in the dark*', raising questions about the delegation of parenting responsibilities to machines (remote parenting). Chaudron also asked whether the technology answers to needs and responds to anxiety, fear and mistrust or, on the contrary, whether it creates needs and contributes to these feelings.

Considering emerging technologies such as wearable sensors, Internet of Things (IoT), and Smart Houses, which are emerging rapidly in a highly connected world, Chaudron sees a narrow border between the *monitoring* and *tracking* of people/children's activities. This border is populated with new technologies including wearable sensors

(accelerometers, temperature, hart-beat, sudation sensors that monitor physical state and activity), home devices linked to the Internet (temperature, humidity, light, movements sensors, intelligent fridges or washing machines linked with remote/software control) and personal belongings (increasingly featuring with geo-localisation monitors).

This may be acceptable when a person monitors his/her own activities and keeps his/her own data. However, it may become a tracking risk when someone 'monitors' a third person's activities and owns these data. In a parent-children relation, introducing such technology may have consequences for *trust*, a fundamental aspect of the education process of raising future independent adult. More deeply still, the technology of Smart-House, wearable sensors and geo-localisation apps challenges the individual's need for *intimacy*and *anonymity* . As 'weak users', children may be among the most affected by this cultural/behavioral change. Monitoring the activities of people or their body state started in hospitals to save lives, and in prisons to protect society. The context of monitoring activities is an important point in considering their acceptability.

These technologies may also affect agency, the capacity to make decisions and assume responsibilities. In the IoT and Smart House context, for example, when machine-learning system can set up the rules of Internet access of the household based upon past activities, or when a fridge proposes menus based upon its users daily physical activities.

However, from the perspective of producers emerging technologies can offer a wide new playground, rich in its possibilities for creation and innovation. Such experiences are open to bottom-up externalization and to personal appropriation of technologies. They place the human back in the centre of the creation. However,, an important consideration remains; how can we create and innovate in a responsible and ethical way? Surveillance technologies may alter the character of one's relationship with others, for example the trust aspects of parents-child relationships. Finally, Chaudron also referred to current demands from companies to have your passwords for social media profiles, pointed toward the notion of "self-quarantine." She described the projects such as those presented by Michalis Vitos, Monica Mendes, Pedro Ângelo and Pablo Rey, as inspiring for educational purposes, in term of creating and playing with data.

6. Insights from the Final Discussion

The workshop allowed a wide range of topics to emerge, even though, due to time constraints, not all areas of interest could be adequately explored.

Most comments coalesced around issues at the core of citizens' veillance. These included: concerns about the use of veillance activities for illegal or controversial purposes; the identification of legitimate goals for citizens' initiatives; the identification of the legitimate technologies, namely their not being intrusive, but respectful for people's lives and freedoms; the requirements for legitimate technologies in terms of their openness, accessibility and usability; the value of DIY as well as of collaborative knowledge and technology in citizens' veillance activities; the potential for collaboration between authorities and citizens in more transparent ways; the recognition of the value of citizen knowledge as knowledge that can be used for publicly relevant activities (e.g. as scientific evidence in courts, in policy decision-making, etc.); the establishment of mechanisms for integrating official and citizen science where the protection of public goods is at stake.

The identification of the limits that should be set to citizens' veillance activities represented a major concern amongst most participants. These concerns, however, touched on a heterogeneous variety of aspects in connection with excessive, improper, unaware, or malevolent uses of ICT, and focused on the risk of discrimination and for increased digital veillance divide.

Several participants were willing to explore DIY technologies in more depth, especially in relation to their social, ethical, and civic implications. In particular, the notion of "commons" was discussed in relation to DIY. Protecting common goods by means of collectively built technological means represents a process where the democratization of power goes hand in hand with building social engagement, commitment, and trust. If participatory procedures have been defined by STS scholar Sheila Jasanoff as "technologies of humility" (Jasanoff 2003), DIY technologies can be seen from this perspective—namely the democratization of science policy-making—as "technologies of trust." Indeed, as some participants noted, practices of "making together" also involve spending time together, getting to know each other, and also learning from each other in a process that can often generate trust amongst those who share the experience.

How and to what extent can these community experiences develop their own economies in order to avoid reliance upon constant subsidisation through volunteer, unpaid work? This question, posed by some participants, touched on the relevant issue of the lasting sustainability of civic projects that cannot only rely on some highly motivated individual effort for their stability and continuity. Indeed, an emerging form of economical perspective and practice that is becoming increasingly relevant and is conquering a number of areas and initiatives is crowdfunding, defined as "the practice

of funding a project or venture by raising many small amounts of money from a large number of people, typically via the Internet." [21] Crowdfunding is often implied in the initiatives of the so-called "low profit" sector, namely organizations producing services or engaging in activities that benefit not only the producer, but also the public.

Participants also raised that DIY methods allow technologies to be experienced in more direct and personal ways, to become integrated in our existences, and technological processes to be re-humanized and individually and collectively re-appropriated.

This is especially true when technology becomes a means for artistic expression. Commenting on the Newton Creek experience (presented by Willis Elkins), for instance, a participant underlined that the technological artistic gaze was able to dignify a wasted and trashed environment by making it perceived as an object of art. Also, technology can provide a way to develop, quantify, and share some form of unexpressed, personal knowledge. For instance, a participant noticed that, while having been accused of a reductionist approach to the body, the language of quantification in Quantified Self (presented both by Adriana Lukas and Anne Wright) has the potential to translate, re-describe, and therefore use and compare, traditional healing cultures (e.g. Ayurvedic medicine) that have been marginalized in Western thought due to their qualitative and non-scientific language.

A further point raised was that, for surveillance to be *participative*, it does not necessarily have to involve any change in the power relations. Indeed, citizens can participate in their own individual or collective surveillance without having any say in the aims, outcomes or procedures involved, and without sharing any of its benefits. As such, in considering participation in any of these senses, which we might associate with this concept of veillance, the term *participative* may not be valuable. Rather, we must pay close attention to the structural and procedural design of surveillance and knowledge generation projects. At its most basic, this means asking questions about the projects' purpose, the actors that control its development and have the power to enact changes to it, and the means of measuring successes and failures. Hakay's framework, which classified the level of participation in citizen science activities, goes some way towards capturing these different levels of participation. The case study from the ExCiteS group, however, also illustrated some of the difficulties involved in implementing a more thoroughly participative model; the participants could not redefine the projects aims or procedural design, other than in ways prescribed in advance by the project. Others, such as the New York waterways project and the Fondazione Bioteca Sarroch emerged from a bottom-up process and, therefore, always defined their own aims and managed to retain this control. However, these cases have

[21] See T. Prive, What Is Crowdfunding And How Does It Benefit The Economy, Forbes 11/27/2012, available at http://www.forbes.com/sites/tanyaprive/2012/11/27/what-is-crowdfunding-and-how-does-it-benefit-the-economy (Accessed 20 August 2014).

also faced problems in gaining the recognition of their legitimacy. Perhaps this is because they were created in response to some injustice and are, therefore, reactive in their character.

Another shared observation concerned the lack of a recognized status for knowledge, and the related technologies, created by citizens. Especially in the domains of health and the environment, the availability of sophisticated of sophisticated means for knowledge production and validation as well as the increasingly common synergies between professional and lay scientists (or scientists and citizens) have deeply transformed bottom-up, non-institutional knowledge, making them very different from older forms of so-called "popular epidemiology" and other epistemic initiatives led by citizens.

Residents of polluted communities have struggled to influence industrial behavior by monitoring the environment for a long time. However, several technological means of surveillance and diverse sources of knowledge– environmental sciences, epidemiology, and genetics– have become available to citizens and have expanded their abilities in the past few years. The sharing of data through ICT platforms and interactive websites is proving crucial in changing the meaning, the scope, and the scale of citizens' initiatives. Moreover, the rapid development of sensors collecting and connecting data from the environment and the body is increasingly enabling Do-It-Yourself organizations.
However, despite all changes in the production and distribution of knowledge and technologies, and in the collaborative initiatives between scientists and citizens, the institutional perception of citizen science and its value seem to be quite limited, and still confined to marginally contributing to official knowledge (EC 2013).

Moreover, several experiences, especially in the field of environmental health (presented by Annibale Biggeri), showed that citizen-driven science is still used in a quite reactive way, namely to restore rights that have been already infringed and violated. Instead, citizens' veillance activities should help monitoring and preventing damage to both health and the environment. Some participants argued that, for knowledge produced through citizens' veillance activities to be proactively used—which implies proactive protection of the rights at stake—, a recognized status and some institutional mechanisms should be put in place.

7. Recommendations

The presentations and the general discussion at the workshop on Citizens' Veillance allowed some reflections that can be translated as draft recommendations for these activities to be legitimately conducted.

Though not specifically aimed to analyze these forms of citizen led initiatives, the Opinion delivered by the EGE on the ethics security and surveillance technologies is a relevant starting point in identifying and proposing the proper conducts and the limits to be established for citizens' veillance. The other main topics addressed here are the following: legitimate goals for veillance activities and rights to be protected; technical and normative requirements for technologies to be used in veillance activities; ….

1. Opinion No. 28 of the EGE (European Group on Ethics in Science and New Technologies): "Ethics of Security and Surveillance Technologies"

EGE Opinion 28 on the ethics of security and surveillance technologies was released on the 20th of May 2014. The document examined and made recommendations on what is the meaning of ethics in the context of security and surveillance, and delivered a few recommendations for the EU, member states, and a range of public and private stakeholders (EGE 2014).

The Snowden case—that took place immediately after the EGE was asked to prepare the new opinion—strongly influenced the structure of the document. Indeed, the main focus of the EGE's reflections concerns the relations amongst national sovereignties, and between sovereign states and their citizens, calling for a renewed public debate on the limits to be placed on security and surveillance technologies, and offers some thoughts on the far-reaching impact of surveillance on trust, privacy, and civil liberties. More specifically, the EGE addressed how to prevent and control pervasive surveillance performed by public authorities beyond the limits of the law, and how to properly enable citizens to react to illegality without violating themselves the law or triggering internal or international crises.

The EGE recognized the legitimate power of democratic stated to use surveillance as a means of safeguarding the security of its citizens, though within the precise limits established by the law.

However, as advances in telecommunications and computing have enabled the data of billions of citizens around the globe to be tracked and scrutinized on an unprecedented scale, the EGE aimed at identifying criteria of accountability and oversight in order to protect the freedom of individuals together with their security.
The EGE discarded the concept and metaphor of the trade-off in balancing freedom and security, namely the idea that some freedom has to be given away in order to achieve security. Instead, the vision of prioritizing rights was preferred and proposed, as it aims at maintaining all rights altogether as a principle, while choosing which right

has to prevail in specific contexts. Indeed, according to this position, no fundamental rights should be given up, but different priorities may be acknowledged under different conditions. "While a proper balance needs to be struck between competing principles or values when they come into conflict, there are some core principles such as human dignity which simply cannot be traded away" (EGE 2014, 87).
As Opinion 28 mostly focused on trust and legitimacy in the interactions between institutions and citizens, civic activities using technologies for veillance and contributing to raise awareness about the protection of common goods or rights were not included in the scope of the opinion. Moreover, amongst other common goods, security can be seen as a goal entrusted to public authorities, and its direct protection by citizens can be very controversial. As already highlighted, security is quite different from goods such as health and the environment, where the moving boundaries between public and private protection have been widely renegotiated, and where a preventative approach is desirable and needed.

Again, bearing in mind the complex implications of the Snowden case, the EGE identified the most proper way for citizens to help checking on the legal use of surveillance technologies by authorities in the establishment of an adequate legal framework for whistleblowing. Opinion 28 urged the European Commission and Member States to ensure that an effective and comprehensive whistle-blower protection mechanism is established in the public and private sectors.

Notwithstanding all these differences, some recommendations proposed by EGE in relation to security and surveillance can be relevant also in the context of citizens' veillance activities.

The EGE recalled the value of dignity and fundamental rights in all activities related to security and surveillance. Rights, the EGE argued, are prioritized rather than traded, while the security and surveillance measures adopted have to be necessary, effective, should respect proportionality, and should be only performed when no better alternatives are available. Moreover, accountability is considered as a necessary pre-requisite for public surveillance, which implies that "surveillance is being undertaken for appropriate reasons and in conformance with publicly available codes of practice;" and the greatest possible degree of transparency should be practiced (EGE 2014, 89).
Also, as to the protection of rights, both "privacy-by design" and "privacy-in design" principles should inform surveillance technologies, namely the "European values of dignity, freedom and justice should be integrated in the design, development and delivery of such technologies" (EGE 2014, 91). To this end, education on the ethical aspects in the design of digital architectures and algorithms should be included in the training of developers (EGE 2014, 90).

All these recommendations can equally and properly apply to citizens' veillance activities and to the technologies used to perform them.

Respect for fundamental rights and for human dignity, as the overall framework for any initiative is obviously paramount, and sets the intrinsic limits of the means and goals for citizens' veillance. Accountability and transparency are crucial elements as well, while "by-design" and "in design" measures are essential expressions of enhanced forms of protection and agency.

2. Legitimate goals and values

The goals that citizens' veillance activities are aimed at have to be legitimate in themselves and legitimate as to the technical means used to pursue them. In other words, both the substantive contents and the processes involved in these activities needs legitimacy and they have to be reflected in the technologies produced and applied.

a) Common goods and legitimate goals: the case for health and the environment

In line with the EGE's recommendations, a rights-based, fundamental values-oriented approach is a necessary requirement in the quest for legitimacy and good practices when surveillance technologies are used by private citizens in performing their activities.

Two mostly uncontroversial values that are good candidates for citizens' veillance activities and that are attracting numerous exercises and experiments are health and the environment. Indeed, health and environment are amongst the most frequent domains for citizens to engage in veillance activities.

There are several reasons explaining this phenomenon. First, health and the environment represent two very basic conditions for life, and constitutionally recognized rights in Europe. Second, they are strictly connected, as a healthy environment is a fundamental requirement for human health. Third, the actual protection of these goods can only be proactive and preventative, and therefore calls for attentive monitoring and veillance. Fourth, a well-established trend exists towards recognizing, both for economic and effectiveness reasons, that health and environmental protection can be fully performed through the direct engagement of citizens.

Other common goods such as security are more controversial. Participatory surveillance for security reasons, as said, raises several concerns, and can be primarily practiced through legitimate forms of collaboration between citizens and authorities.

b) Forms of participation in surveillance

As discussed, citizens can participate in their own individual or collective surveillance without necessarily sharing in its benefits. We must pay close attention to the structural and procedural design of surveillance and knowledge generation projects.

At its most basic, this means asking questions about the projects' purpose, the actors that control its development and have the power to enact changes to it, and the means of measuring successes and failures.

Many of these difficulties may arise in the problem definition phase. Where the problem is defined externally and brought to participants, a power structure is introduced from the outset and this may be difficult to transform. Even where a citizen science or participative surveillance project is designed for empowerment, the protection of rights, they may be born into a context of conflict and controversy and, therefore, forged in a space where mistrust reigns and the benefits of the project are already too late for the early victims of injustice.

Establishing the recognition of other forms of knowledge through a situation of mutual trust and respect may require a generation of projects that are proactive in their inception.

c) Reactive v. proactive: "rights from wrongs" or "rights before wrongs" ?

The wide variety of forms for sur- sous- and self-veillance calls for a scrutiny of the criteria justifying their legitimacy. Some cases and experiences illustrated above seem to (implicitly) derive their legitimacy from the need to restore a "right" after a "wrong" had happened; others are started as ways to raise awareness for increased and proactive empowerment in protecting some goods; others tend to make individuals—and communities of individuals—empowered in their autonomous abilities to protect their own health.

Often, and with different degrees, some institutional obligations such as protecting and implementing constitutional rights, or controlling the quality of environmental and health data to comply with established pollution levels, have been violated. In other words, institutional and legal mechanisms were not strong or reliable enough to grant citizens' rights.

Therefore, a possible rationale for legitimate participatory surveillance can depend on its contributing to re-establish a lawful condition. Also, the means adopted should not infringe other persons' rights, being based on surveillance of environmental components and on self-surveillance. Finally, industry is not excluded from an open collaboration where the conditions exist.

Whereas revisions of all surveillance exercises seem highly desirable, participatory surveillance projects led by citizens should meet some criteria of legitimacy to be performed. These "vigilance" projects – a term less negatively loaded than surveillance – have the potential to become complementary (and hopefully preventative) means

for law implementation where citizens' rights have been violated and are difficult to restore.

3. Legitimate technical means

a) Open paradigm for citizen knowledge production

The means for citizens to perform their own watching activities towards the production of socially useful and empowering knowledge, depend on the ability to assure principles of transparency, accessibility and participation in those same means. Such ability is developed taking inspiration from open source models, where all data as the source code, blueprints and other documentation, is available at no cost to the public for redistribution, use and improvement. In addition, a commons based rationale for peer-to-peer collaboration is particularly relevant, in situations where shared goods or resources are jointly developed and maintained by a community. An open framework overtly places in the civic realm the decisions to define who produces the data, who owns it, who can access and use it, and who draws value from it. Emerging citizen-based initiatives are thus centered on the issues of public infrastructures for communication, unrestricted access and use of raw data, or decentralized control through online open platforms, licenses, databases, servers, domains. This open paradigm doesn't overlook, however, in most instances the creation of clear Terms of Use, and data protection and privacy policies that are discussed and defined within the communities in question. Overall, it is increasingly demonstrating its validity in terms of promoting co-responsibility in collecting, checking and interpreting data, and in fostering new forms of accountability between citizens and public and private sectors.

b) DIY and making

Accessibility of digital manufacturing tools (3D printers, CNC machines, laser cutters, open source electronics, etc.) coupled with multiplying fabrication spaces and online communities providing support to anyone interested in "making something", are ushering in new possibilities for bottom-up approaches to pursue and develop their aims. It can cover a large spectrum of initiatives, from more individually oriented, for instance tracking your private home environment or your household for security purposes, to community or grassroots oriented, for example monitoring environmental data in your neighborhood or asserting sources of pollution in specific geographical areas. The main notion to be retained is that, through DIY and making, citizens and communities have increasingly at their disposal concrete venues to reflect upon, to select what they consider the best options, and even to create their own technological solutions tailored to their needs, social contexts and objectives. This direct engagement with the acts of fabricating or producing artifacts can enhance in certain cases a sense of empowerment, agency, personal and social autonomy, and further stimulate news means of civic intervention in spheres of institutional power.

c) Rights in-design

By-design forms of values and rights protection within digital architectures imply a top-down, quite paternalistic vision, where pre-defined, often black-boxed technical measures prevent individuals from experiencing some harms. A different approach consists in looking at choices made within the system as a matter of individual agency and, at least prospectively, as a matter of "rights" for citizens, invested of an active role in using, experiencing, and controlling their options, powers, privacy, and data. The overall reiterated process of actively framing and tailoring the choices embedded in a technological system not only triggers a more aware and responsible agency but, as forms of collaborations with other citizens/users (and also data controllers) are also involved, generates trust and ongoing, renewed trustworthy relations.
This approach aimed at granting "rights-in-design" considers digital architectures as a place for citizens' (moral and legal) entitlements.
In Opinion 28, as said, the EGE has endorsed this active and proactive perspective that, on the one hand, makes citizens empowered towards the digital world; and, on the other hand, makes them also more responsible for their choices.

d) The role of Citizen Science
According to the Green Paper on Citizen Science (EC 2013), the concept of Citizen Science has been defined in many different ways. A shared element concerns the link between the general public and scientific research in order to find answers to real-world questions. Besides this, different definitions highlight elements that are also illustrative of the evolution of the field. Indeed, some understand "Citizen Science as an approach, which involves volunteers from the general public in scientific investigations during data collection and analysis. Others define it more broadly, as the public participating in scientific research, which includes also scientific activities like the asking of questions, formulation of hypotheses, interpretation of results. Current discussions around the definition of citizen science not only focus on the scope of activities but also what to understand under "volunteers" and how to composite citizen science teams: (EC 2013, 21). What still seems to be lacking is a single generally accepted definition of citizen science.

Most experiences presented at the workshop, however, displayed models that show a further development. The case of PM2.5 in Florence (presented by Annibale Biggeri), for instance, revealed a situation where citizens are *de facto* working, together with scientists and lawyers, on

innovative forms of reliable knowledge production as potential templates to be followed by institutions in order to re-gain credibility. Indeed, the new hybrid communities of scientists, lawyers, and citizens are not competing or fighting against institutions; instead, they are proposing the most updated ways of creating robust knowledge for public policy purposes. In other words, they are suggesting to institutions how they should work to be trusted by citizens.

The PM2.5 case has shown a recipe for trusted public knowledge, as it encompassed a variety of scientific and civic elements: a collaboration between citizens and scientists (or lay and professional scientists) to define the scientific issues and location of monitoring devices; validation of results; implementation of a website for continuous monitoring open and meaningful for citizens. As it has been suggested, two other elements should be added to enhance the quality of the project, namely the crowdfunded purchase of monitoring devices and the creation of an open platforms providing access to raw data. [22] Crowdfunding as a requirement for best practices in citizens' veillance initiatives emerged frequently during the workshop. As transparency and accountability are essential elements in making these citizens' activities legitimate, the source of funding, as well as the amount of each contribution, are critical in generating trust.

The current understanding of, and role for, Citizens Science at institutional level does not seem to be equipped neither to receive nor to help these new developments.
Part of what we have called above "reactive" role of citizens' veillance activities also depends from the fact that, in several contexts, the main way for Citizens Science to emerge is through conflicts, court decisions, and confrontation with officially produced knowledge—or, as in some in environmental disasters, hidden knowledge.

A different appreciation of Citizen Science at institutional level and the preparation of strategies of effective integration are therefore needed.

[22] G. Bindi, Misuriamo lo smog, Terra Nuova 296, luglio-agosto 2014, available at http://www.aamterranuova.it/ (Last Accessed 22 August 2014).

References

Agamben, G. 2005. State of Exception. Chicago IL:Chicago University Press (2003).

Albrechtslund, A. 2008. Online Social Networking as Participatory Surveillance. First Monday 13 (3). http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949.

Anderson, C. 2012. Makers: The New Industrial Revolution. New York: Crown Business.

Arendt, A. 1998. The Human Condition, Chicago IL:University Of Chicago Press (1958).

Art.29 WP (Article 29 Working Party) (2009), Opinion 168 on The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.

Borgmann, A. 1987. Technology and the Character of Contemporary Life: A Philosophical Enquiry. Chicago: University of Chicago Press.

Burke, A. 2007. What security makes possible: some thoughts on critical security studies, Working Paper 2007/1, Australian National University, Canberra, http://ips.cap.anu.edu.au/ir/pubs/work_papers/07-1.pdf (Accessed 14 May 2013).

Cascio, J. 2005. The Rise of the Participatory Panopticon. 4 May, http://www.worldchanging.com/archives/002651.html

C.A.S.E. Collective. 2006. Critical Approaches to Security in Europe: A Networked Manifesto, Security Dialogue 37, 443-487.

Dershowitz, A.M. 2004. Rights from Wrongs: A Secular Theory of the Origin of Rights. New York:Basic Books.

EC (European Commission) 2013. SOCIENTIZE Project to the European Commission's Digital Science Unit. Green paper on Citizen Science for Europe: Towards a society of empowered citizens and enhanced research http://ec.europa.eu/digital-agenda/en/news/green-paper-citizen-science-europe-towards-society-empowered-citizens-and-enhanced-research-0 (Accessed 20 August 2014)

EDPS, European Data Protection Supervisor. 2010. Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy (Opinion on Privacy By Design). OJ C 280, 16.10.2010, 1–15.

EGE, European Group on Ethics in Science and New Technologies. 2014. Opinion 28 of the European Group on Ethics in Science and New Technologies, Ethics of Security and Surveillance Technologies, Brussels, 20 May 2014.

Eglash, R., Crossiant, J., Di Chiro, G. and Fouché, R. 2004. Appropriating Technology: Vernacular Science and Social Power. Minneapolis: University of Minnesota Press.

Foucault, M. 1995. Discipline and Punish: the Birth of the Prison, New York: Random House (1975).

Gershenfeld, N. 2007. Fab: The Coming Revolution on Your Desktop--from Personal Computers to Personal Fabrication. New York: Basic Books.

Hatch, M. 2014. The Maker Manifesto: Rules for Innovation in the New World of Crafters, Hackers and Tinkerers. New York: McGraw-Hill.

Henckel von Donnersmarck, F. 2007. Das Leben der Anderen: Filmbuch, Frankfurt: Suhrkamp.

House of Lords. 2009. Select Committee on the Constitution, Surveillance: Citizens and the State, Volume I: Report, 2nd Report of Session 2008–09, 6 February, London: The Stationery Office Limited.

Huey, L. and Fernandez L.A. (Guest editors). 2009. Special issue: Surveillance and Resistance Surveillance & Society. 6(3).

Ihde, D. 1990. Technology and the Lifeworld: from Garden to Earth. Bloomington: Indiana University Press.

Jacobs, J. 2012. Your phone will soon be your new doctor, Sep. 30, http://gigaom.com/2012/09/30/your-phone-will-soon-be-your-new-doctor/

Jasanoff, S. 2003. Technologies of Humility: Citizen participation in governing Science. Minerva, 41: 223–244.

Kroes, N. 2011. Internet essentials, OECD High Level Meeting on the Internet Economy, Paris, 28 June.

Kroes, N. 2013. Using cybersecurity to promote European values. Launching the EU's Cybersecurity Strategy press conference /Brussels, SPEECH/13/104, 7 February.

Lyon, D. 2007. Surveillance Studies: An Overview. Cambridge, UK: Polity.

Mann, S., Nolan J. and Wellman B. 2003. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. Surveillance & Society 1(3): 331-355.

Marx, G.T. 2002. What's New about the "New Surveillance"? Classifying for Change and Continuity. Surveillance & Society 1(1):9-29.

Marx, G.T. 2007. Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information --"Hey Buddy Can You Spare a DNA?" Ann Ist Super Sanità 43, 1: 12-19.

Nissenbaum, H. 2009. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Palo Alto (CA):Stanford Law Books.

Ottinger, G. 2010. Constructing Empowerment Through Interpretations of Environmental Data.
Surveillance & Society 8(2): 221-234.

Pereira, A.G. and Tallacchini, M. 2014. Governance of ICT Security: A Perspective from the JRC, Technical Report, Luxembourg: Publications Office of the European Union.

Ratto, M. and Boler, M. eds. 2014. DIY Citizenship: Critical Making and Social Media. Cambridge and London: The MIT Press.

Sennett, R. 2009. The Craftsman. New Haven: Yale University Press.

UNDP (1994), Human Development Report 1994, Oxford, Oxford University Press.
van den Hoven J., Weckert J. (2008), Information Technology and Moral Philosophy, Cambridge University Press 2008.

Vaz P. and Bruno F. 2003. Types of Self-surveillance: from abnormality to individuals at 'risk,' Surveillance & Society 1(3):272-291.

Weitzman E.R., et al. (2013), Participatory Surveillance of Hypoglycemia and Harms in an Online Social Network, JAMA Internal Medicine 173, 5, March 11, 345-351.

Annex - Agenda

March 20th 2014 - Building 36b, Room 3

14.00 - 14.30
Welcome by Jean-Pierre Nordvik (JRC – Ispra, Italy)
Introduction to the Workshop by Angela G. Pereira, Mariachiara Tallacchini, Philip Boucher, Susana Nascimento (JRC – Ispra, Italy)

Session 1 – ICT, Values, and Rights for Citizens' Veillance
14.30 - 17.30

- Helen Nissenbaum (New York University, NY, USA) Respect for Context as a Benchmark for Privacy: What it is and isn't
- Anders Albrechtslung (Aarhus University, Aarhus, Denmark), Participatory - Surveillance for Citizens' Veillance and Empowerment
- Jim Dratwa (BEPA, European Commission), Reframing Security and Surveillance Technologies: Ethical Experimentations of Europe

17.30-18.00 General discussion

March 21st - Building 36b, Room 3

Session 2.1 – Experiences using ICT for Citizens' Veillance: Research Groups
09.00 - 10.15

- Michalis Vitos (UCL, London, UK), Taking Citizen Science to Extremes: from the Arctic to the Rainforest
- Fivos Andritsos (JRC – Ispra, Italy), Future Surveillance: The Citizen in the Loop or in the Loupe?

Session 2.2 – Experiences with ICT for Citizens' Veillance: Environment, Health, and Bodies
10.30 - 12.30

- Annibale Biggeri (University of Florence, Florence, Italy), ICT and Genetics to Empower Citizens' Health
- Willis Elkins (Newtown Creek Alliance, New York, NY, USA), Citizen Surveying within Polluted Areas
- Adriana Lukas (Quantified Self, London, UK), The Self in Quantified Self: A Perspective on Personal Data Autonomy

Session 3 – Experiences using ICT for Artistic Civic Science
13.30 - 14.30

- Mónica Mendes (University of Lisbon and M-ITI, Portugal) and Pedro Ângelo (void.io, Portugal), Appropriating Video Surveillance for Art and Environmental Awareness: Experiences from ARTiVIS Project
- Pablo Rey (Public Lab and Basurama, Spain), DIY Balloon Mapping Workshops in Spain: Documenting the Territory and Community Building

Discussion Session - Normative Issues, Technological Solutions, Research Perspectives
14.30 – 16.30

- Invited Discussants: Anne Wright (Carnegie Mellon, Pittsburgh PA, USA); Apostolos Malatras (JRC – Ispra, Italy); Stéphane Chaudron (JRC – Ispra, Italy)

General Discussion

16.30 Closing Remarks

European Commission
EUR 26809 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: Emerging ICT for Citizens' Veillance: Theoretical and Practical Insights

Author(s): TALLACCHINI Mariachiara, BOUCHER Philip, NASCIMENTO Susana.

Luxembourg: Publications Office of the European Union

2014 – 55 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-39775-2

doi: 10.2788/11828

LB-NA-26809-EN-N

JRC Mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

Serving society
Stimulating innovation
Supporting legislation

doi: 10.2788/11828

ISBN: 978-92-79-39775-2