Sci Eng Ethics (2018) 24:821–830
https://doi.org/10.1007/s11948-018-0039-z

EDITORIAL

Emerging ICT for Citizens' Veillance: Theoretical and Practical Insights

Philip Boucher[1] · Susana Nascimento[2] · Mariachiara Tallacchini[3]

Received: 22 February 2018 / Accepted: 23 February 2018 / Published online: 28 February 2018

Abstract In ubiquitous surveillance societies, individuals are subjected to observation and control by authorities, institutions, and corporations. Sometimes, citizens contribute their own knowledge and other resources to their own surveillance. In addition, some of "the watched" observe "the watchers" "through" sous-veillant activities, and various forms of self-surveillance for different purposes. However, information and communication technologies are also increasingly used for social initiatives with a bottom up structure where citizens themselves define the goals, shape the outcomes and profit from the benefits of watching activities. This model, which we define as *citizens' veillance* and explore in this special issue, 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.

Keywords Surveillance · Citizens' veillance · Emerging ICT

✉ Philip Boucher
philip@bouch.eu

Susana Nascimento
susana.nascimento@ec.europa.eu

Mariachiara Tallacchini
mariachiara.tallacchini@unimi.it

[1] European Parliament - European Parliamentary Research Service, Brussels, Belgium

[2] European Commission - Joint Research Centre (JRC), Brussels, Belgium

[3] Facoltà di Economia e Giurisprudenza, Università Cattolica S.C., Piacenza, Italy

Introduction: Towards Citizens' Veillance

In ubiquitous surveillance societies, individuals are subjected to observation and control by authorities, institutions, and corporations. Sometimes, we observe citizens contributing their own knowledge and other resources to their own surveillance. We also see some of 'the watched' observing 'the watchers' through sous-veillant activities, and various forms of self-surveillance for different purposes (Lyon 2007). However, information and communication technologies (ICT) are also increasingly used for social initiatives with a bottom up structure where citizens themselves define the goals, shape the outcomes and profit from the benefits of watching activities. This model, which we define as *citizens' 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.

Here, we use this concept of citizens' veillance to explore a set of activities performed by citizens—often under the banner of citizen science (CS) and peer collaborative knowledge—with the broad and primary aim of producing knowledge that is socially useful and empowering, in contrast with other watching activities that are mobilised as a means of control. We understand citizens' veillance as a condition in which citizens' cognitive alertness and knowledge production is proactively oriented towards the protection of shared goods. Our reasons to adopt the term veillance relate to the elimination of the locations and directions of the inquisitive "gaze"—the 'sur-', 'sous-' and 'self-'—toward a broader "becoming aware" of the surrounding context. We also seek to emphasise shifts from control to cognition, from power to alertness. Three types of outcome can be identified: First, the collective production of knowledge which is usually the most immediate objective of the watching activity; second, the practical and social impact of the production and mobilisation of this knowledge; and, third, the broad defence of fundamental rights and values. Citizens' veillance may result in forms of knowledge that can be mobilised to complement, implement, and sometimes confront institutional or corporate knowledge production. In 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 represents a strategy for improved protection of citizens' rights.

These activities, however, raise several epistemic and normative issues. From the epistemic point of view, it is relevant that knowledge production processes are no longer limited to authorised scientific communities and officially designated spaces but can now take place everywhere in society. We see increased merging and converging between scientific, artistic and citizen communities and, now, a wider range of non-conventional actors can produce relevant, reliable and transparent knowledge that can complement or confront traditional, conventionally produced knowledge. For example, communities can mobilise a combination of increasingly accessible ICT, tools and epistemic frameworks to expand their margins of control over their health and the environment. Health and the environment represent two major historical domains and social values, constitutionally

protected in several countries, which civic and community activities have targeted through watching activities even before the wide availability of ICT skills and tools. Now that these are increasingly available to a wider range of people, we see more citizens' veillance targeting the protection of such common goods, often restoring rights or preventing their infringement through the creation of knowledge, spreading of awareness and sharing of data and results.

From both an epistemic and a normative perspective, knowledge is collectively peer-generated by means of individually accessible and, often, do-it-yourself (DIY) ICT. However, not all ICT are alike: the technologies used to perform these activities range from web platforms to portable and wearable sensors, to drones and open source surveillance and mapping kits. They vary significantly in their accessibility, usability, degree of invasiveness and pervasiveness, and their criteria for openness and transparency. For such knowledge generation activities to gain democratic legitimacy and to re-draw its boundaries with traditional knowledge production, the social values promoted by these initiatives should be reflected in the democratic and transparent character of ICT architectures.

An Open and Legitimate Paradigm for Citizen Veillance: Goals and Technical Means

Citizens' veillance systems have to address common issues in relation to their values and goals as well as to the degree of openness of the digital architectures and ICT used and implemented. The aims of citizens' veillance activities have to be legitimate in themselves, and also in terms of the technical means used to pursue them. In other words, both the substantive contents of the activity and the set of processes and tools that are developed and deployed to implement it need to be legitimate and internally commensurable.

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. Contemporary critical studies in security and surveillance (CSS), especially in Europe, have deeply scrutinized practices of watching and controlling citizens, proposing a vision primarily centred on human beings and their fundamental rights as individuals, with human emancipation as its central concern (CASE 2006). The United Nations launched in 1994 (and re-proposed in 2012)[1] the concept of "human security", namely that security should focus on human beings, not sovereign States, and should consider individuals' and communities' well-being as criteria for legitimacy. This rights-based and fundamental 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

[1] United Nations Development Programme, Human Development Report 1994, Oxford, Oxford University Press; United Nations General Assembly, Follow-up to Paragraph 143 on human security of the 2005 World Summit Outcome, 25 October 2012.

activities. The existence of these conditions is proposed here as the threshold for considering the social acceptability of these activities.

As for the technical means for citizens to perform their own watching activities towards the production of socially useful and empowering knowledge, their legitimacy depends upon their ability to ensure the principles of transparency, accessibility and participation. An open framework overtly positions the decisions about who produces the data, who owns it, who can access and use it, and who draws value from it into the civic realm. Emerging citizen-based initiatives are thus centred on the issues of public infrastructures for communication, unrestricted access and use of raw data, or decentralised control through online open platforms, licenses, databases, servers, domains. In most cases, these open paradigms do not overlook the creation of clear terms of use, data protection and privacy policies but these are discussed and defined within the communities of users in question. Overall, it increasingly demonstrates 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. Moreover, these technological requirements are now increasingly coupled with open forms of funding, namely crowdfunding, as the economic counterpart of the independency and trustworthiness of a proposed initiative.

Certain aspects involved in citizens' veillance activities require further clarifications. In the following section, we offer some reflections on the main topics addressed so far by citizens' veillance activities—health and the environment—in particular their substantive goals, their technical means and the criteria for their legitimacy.

Health and the Environment

It seems that the interconnected fields of health and the environment represent the most frequent domains for citizens to engage in veillance activities and are perhaps, for the moment, the most socially, ethically, and legally promising applications areas. We suggest four reasons why this might be the case: First, health and the environment represent two very basic conditions for life, and constitutionally recognized rights in many countries; second, they are strictly connected, as a healthy environment is a fundamental requirement for human health; third, the actual protection of these goods should preferably be preventative, calling for proactive monitoring and veillance and; 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.

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 their rights and

to exert them by transforming knowledge and technology into civil and community life.

The Role of Citizen Science

CS has become paramount in co-creating knowledge about health and the environment. The concept of CS has been defined in many different ways (EC 2013). A shared element concerns the link between the general public and scientific research in order to find answers to real-world questions. However, some understand CS 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, and interpretation of results. Current discussions around the definition of CS not only focus on the scope of activities but also how to understand the role of "volunteers" and how to compose CS teams (European Commission 2013, 21). What still seems to be lacking is a single, comprehensive and generally accepted definition.

As we shall see in some of the experiences presented in this issue, some citizens' veillance activities reveal further development: for instance, citizens 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 but, instead, proposing alternative approaches to the creation of robust knowledge for public policy purposes. In other words, they are suggesting how institutions can work in a way that can be trusted by citizens.

The current understanding of, and role for, CS at institutional level is still far from being equipped to help these new developments. Still, the main way for CS to emerge is through conflicts, court decisions, and confrontation with officially produced knowledge. A different appreciation of CS at institutional level and the preparation of strategies of effective integration is therefore needed. Encouraging signs are coming from the U.S. Office of Science and Technology Policy, which since September 2015 has pushed federal agencies to incorporate CS and crowd funding into their programmes (Holdren 2015). An operational plan has implemented a set of measures, including basic guidelines for effective use, appointment of agency coordinators, public database of projects, and a Federal Crowdsourcing and CS Toolkit[2] to design, carry out, and sustain effective projects. This political acknowledgement of CS will be monitored closely by the European Commission.

[2] https://crowdsourcing-toolkit.sites.usa.gov/.

DIY and Maker Approaches

In the past few years, we have been witnessing the rise of DIY and making approaches, which call 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, or other types of labs.

On one hand, a set of tools and machines is becoming more accessible for users/citizens/groups/communities to design and manufacture artefacts (objects, systems, networks or applications), such as digital fabrication devices (including design software, laser cutters, 3D printers etc.), open source and low-cost hardware (Arduino, Raspberry Pi, and others), or even smartphones and smart devices. On the other hand, now data and documentation are widely available online, such as schematics, circuit layout, code, 3D models, electronics tutorials and support materials, together with online communities for exchanging experiences, sharing their work, and supporting others with common interests. These provide access to other people and communities, digital fabrication, electronics and other ICT tools for rapid prototyping, under a common rationale that any user, consumer, or citizen can ultimately produce, use, share, copy and improve objects, systems or devices. 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 science and technology.

Empowerment can be connected to practical possibilities for users to embed values, norms and expectations in artefacts themselves, so they can be better integrated in particular realities and contexts. Access to tools and machines allows for more open processes to design, modify and create artefacts. By opening up such processes, a greater variety of options and choices are made more accessible in their purposes, impacts and uses of the artefacts in question, regarding for instance personal health issues, pollution in local areas, 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.

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 artefacts, citizens are at the same time embedding their values and expectations in artefacts, and regaining degrees of power and control over technology itself. The search of new forms of technological action (Eglash et al. 2004) is visible 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). The most relevant aspect of DIY and making approaches is a renewed acknowledgement of questions such as education, power, development, equality or gender, in citizens' lives and in their potential disruptions of material and online worlds.

Rights in the Design of Digital Architectures

Already in 1980 Langdon Winner pointed out that all machines, structures and technical systems should not only be analysed 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 have led to a number of developments in ICT to make them more "human-centred", and have raised awareness about the choices implicitly embedded, packed, and black-boxed in programs and devices. Today, it is well recognized that all algorithms embody rules and decisions in their own designs and structures (Hildebrandt and Rouvroy 2011), and there is a trend toward making these normative choices explicit, transparent, discussed, and controllable, from designers and engineers to institutions and citizens. The paradigm of openness connected to citizen veillance technologies is part of this trend and is committed to transforming digital architectures into sites for transparent deliberations as a matter of democratic legitimacy and citizens' rights.

Indeed, a variety of technological measures have been created and implemented to protect individual rights, and especially privacy, "by design", namely by embedding these algorithms within the ICT architectural structures (Cavoukian 2009). However, a different, or at least complementary, approach is needed to raise awareness about the processes through which values and norms become embedded in technological architectures. This approach, aimed at empowering users/citizens in the design of digital architectures, implies opening up and making available to them some relevant choices in the algorithms as a matter of legal entitlement.[3]

If the "by-design" approach delivers the protection of rights, privacy and data within the product itself, the "in-design" approach opens digital architectures up to users, which also implies a shift in understanding privacy as a "right", rather than as a paternalistic legal protection (Pereira and Tallacchini 2014). By-design protection implies a top-down paternalistic vision, where pre-defined, often black-boxed, technical measures prevent individuals from experiencing some harms. In-design approach consists in looking at choices made within the system as a matter

[3] 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).

of individual agency and, at least prospectively, as a place for citizens' (moral and legal) entitlements (Lunshof et al. 2014). The overall reiterated process of actively framing and tailoring the choices embedded in a technological system not only triggers more aware and responsible users but, as forms of collaborations with other citizens/users (and also data controllers) are also involved, generates trust and ongoing, renewed trustworthy relations (Kounelis et al. 2014). This approach 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 on the relationships between technology and ethical and legal choices.

A Special Issue Mixing Academic and Non-academic Contributions

We held a workshop on "Emerging ICT for Citizens' Veillance" on March 20–21, 2014 at the European Commission's Joint Research Centre (JRC), Ispra, Italy. 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; and 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. This Special Issue gathers contributions from the invited participants to this workshop and focusses upon five main questions:

- How do these new forms of peer-production or citizens-led production of knowledge redefine 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? How should values- and rights-in-design 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?
- Through which processes can authorities, policymakers, industry, civil society organizations, users, and communities interact and intervene in ICT orientation?
- What are the main challenges arising from the use of DIY and open source tools which are used to empower citizens and communities to create and share data in a collaborative logic and to provoke transformations in their practices?

The workshop and this resulting Special Issue in the Journal of Science and Engineering Ethics reflect in many ways the profile of citizens' veillance activities. In the same way as citizens' veillance activities position different kinds of actors at the centre of knowledge production activities, the workshop and resulting Special Issue bring citizens, activists and artists together in spaces that is normally dominated by scholars and policymakers. We see the strength of the initiative in its variety of contributions, combining traditional analyses of an academic style with accounts

from actors engaged in citizen veillance activities. It follows, however, that some of the contributors to the Special Issue often fall outside the norms of scholarship that are usually found in academic journals. We identify two types of contribution: Scholar-led articles which focus in some way upon citizens' veillance activities and practitioner-led articles which focus upon their experiences in carrying out these activities.

Among the scholar-led articles, Helen Nissenbaum argues for the approach of contextual integrity as an underlying justificatory, or normative rationale, to protect privacy in an increasingly information-mediated world. Tjerk Timan and Anders Albrechtslund provide a systematic scholarly enquiry on surveillance practices and tracking technologies, empirically grounded in smartphone users' everyday experience in the nightlife district of the city centre of Rotterdam. Within the area of public health, Mariachiara Tallacchini and Annibale Biggeri engage in a review of peer production of knowledge, focusing on two Italian initiatives where citizens and scientists worked together with the goal of protecting environmental health in potentially highly polluted contexts. Also within healthcare, Lucia Vesnic-Alujevic, Melina Breitegger and Ângela Guimarães Pereira offer a discussion on DIY practices with a focus on the online communities of Fitbit and the Quantified Self movement and their users' knowledge claims, shared experiences and imaginations about wearable sensors. In the broader domain of the Internet of Things (IoT), Gianmarco Baldini, Maarten Botterman, Ricardo Neisse and Mariachiara Tallacchini present a new framework for privacy based on Ethical Design, which grants wider a more active role for citizens to control their personal data. Susana Nascimento and Alexandre Pólvora explore the assumptions and challenges of maker cultures for pushing forward technological action, defined as active and critical interventions within everyday life, through snapshots on particular maker contexts.

Among the practitioner-led articles, Monica Mendes, Pedro Angelo, Valentina Nisi and Nuno Correia present their ongoing collaborative research project, ARTiVIS, mixing technological and artistic explorations with activism and experiments with real-time video, DIY surveillance technologies and sensor data for environmental awareness. Within the community around the Public Laboratory for Open Technology and Science (Public Lab), Don Blair, Catherine D'Ignazio, Shannon Dosemagen, Hagit Keysar and Pablo Rey Mazón explore use cases of DIY, open source, accessible and community-built technologies developed within the diverse array of topics—aerial mapping, water quality monitoring and civic science. As a co-founder of the BodyTrack project, an open source web service, Anne Renee Wright offers an account of her personal experience in self-tracking as a practice of individual empowerment to explore and address health and wellness issues.

References

Cavoukian, A. (2009). *Privacy by design. The 7 foundational principles*. https://www.privacybydesign.ca/index.php/paper/privacy-by-design/. Accessed 15 January 2016.

Eglash, R., Crossiant, J., Di Chiro, G., & Fouché, R. (2004). *Appropriating technology: Vernacular science and social power*. Minneapolis: University of Minnesota Press.

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 15 January 2016.

European Group on Ethics in Science and New Technologies. (2014). Opinion 28 of the European Group on ethics in science and new technologies. In *Ethics of security and surveillance technologies.* Luxembourg: Publications Office of the European Union.

Hildebrandt, M., & Rouvroy, A. (Eds.). (2011). *The philosophy of law meets the philosophy of technology. Autonomic computing and transformations of human agency*. London: Routledge.

Holdren, J. (2015). *Addressing societal and scientific challenges through and crowdsourcing.* Memorandum Office of Science and Technology Policy, September 30. https://www.whitehouse.gov/sites/default/files/microsites/ostp/holdren_citizen_science_memo_092915_0.pdf. Accessed 15 January 2016.

Kounelis, I., Baldini, G., Neisse, R., Steri, G., Tallacchini, M., & Pereira AG (2014). Building trust in human–internet of things relationship. *IEEE Technology and Society Magazine, 33*(4), 73–80.

Lunshof, J. E., Church, G. M., & Prainsack, B. (2014). Raw personal data: Providing access. *Science, 343*(6169), 373–374.

Lyon, D. (Ed.). (2007). *Surveillance studies: An overview*. Cambridge: Polity.

Pereira, A. G., & Tallacchini, M. (2014). *Governance of ICT security: A perspective from the JRC, technical report*. Luxembourg: Publications Office of the European Union.

Ratto, M., & Boler, M. (Eds.). (2014). *DIY citizenship: Critical making and social media*. Cambridge and London: MIT Press.

Winner, L. (1980). Do artifacts have politics? *Daedalus, 109*(1), 121–136.