CHAPTER 2

SCIENCE, ETHICS, AND RESPONSIBLE RESEARCH – THE CASE OF SURVEILLANCE

Alfonso Alfonsi and Maresa Berliri

ABSTRACT

This chapter, based on a sociological approach, addresses the ethical issues of surveillance research from the perspective of the profound transformations that science and innovation are undergoing, as part of a broader shift from modern to post-modern society, affecting also other major social institutions (such as government, religion, family, and public administration). The change occurring in the science and technology system is characterised by diminishing authority, uncertainty about internal mechanisms and standards, and a declining and increasingly difficult access to resources. Such changes, also related to globalisation and new digital technologies, have transformed the way research is conducted and disseminated. Research is now more open and its results more easily accessible to citizens.

Scientific research is also put under increased public scrutiny, while, at the same time, public distrust and disaffection towards science is rising. In such a context, it is more important than ever to make sure that research activities are not compromised by fraudulent and unethical practices. The legitimate expectations of citizens to enjoy their rights, including the ability to protect their private sphere, are growing. Scientific and technological development is deeply interrelated with the widespread awareness of these rights and the possibility of exercising them, but it produces also new risks, while a widespread sense

Ethical Issues in Covert, Security and Surveillance Research
Advances in Research Ethics and Integrity, Volume 8, 17–28

ISSN: 2398-6018/doi:10.1108/S2398-601820210000008003

of insecurity increases. The digital revolution, while improving people's quality of life, offers at the same time new opportunities for crime and terrorism, which in turn has produced a demand to strengthen security systems through increasingly advanced and intrusive surveillance technologies. Misconduct in the field of surveillance may not only undermine the quality of research, but also further impair society's trust in research and science as well as in the State and its institutions.

Keywords: Surveillance; sousveillance; ethics; security; social sorting; surveillance creep; privacy; trust

INTRODUCTION

Following a sociological perspective, which accounts for the overarching shift from modern to post-modern society, this chapter focusses on the current efforts to find a balance between two equally compelling social demands: that of security and that of protection of personal rights, including privacy. In particular, the social costs of surveillance are addressed, together with efforts to minimise them. In this regard, the debate about contentious topics, such as social sorting, surveillance creep, data slippage, dual use and the like are examined to highlight the effects that inappropriate surveillance practices can have in harming individuals and social groups. In a broader perspective, the effect that such kinds of improprieties can have in diminishing social trust are discussed with regard to the challenges to the authority of both the State and scientific institutions. To this end, we will discuss the merit of broad conceptualisations of surveillance, such as the notion of 'surveillance society' advanced by the Surveillance Studies Network, or David Lyon's (2018) 'surveillance culture'. This broad view will be confronted with the more restricted definitions of surveillance focussed on activities specifically targeted for law enforcement and crime prevention, with the massive use of digital technologies (smart systems) and large amounts of data, both ad hoc and for other purposes. On the other end of the spectrum, we will also examine the implications of the fact that new digital technologies allow more and more citizens to perform a 'bottom up' surveillance activity with regard to the behaviour of public officials, including law enforcement agents.

SURVEILLANCE IN THE CONTEXT OF POST-MODERN SOCIETY

Addressing the ethical issues of surveillance from a sociological point of view requires placing such reflection in the context of the profound transformation that science and innovation are undergoing as part of the shift from modern to post-modern society that is affecting all social institutions. In fact, at the core

of current surveillance activities is the massive use of different kinds of technologies, including ICTs,[1] in fields where research and innovation are moving and evolving at an extremely fast pace. This ongoing transformation has been described and conceptualised in different ways by scholars and researchers, like the shift from Mode1 to Mode2 scientific production (Gibbons et al., 1994), post-academic research (Ziman, 2000), or triple helix innovation model (Etzkowitz & Leydesdorff, 2000; Leydesdorff & Etzkowitz, 1998). Some of its features, however, tend to be highlighted in a similar way by many authors (d'Andrea, 2019; Nowotny, Scott, & Gibbons, 2001).

- Science and innovation are becoming a multiactor process, involving a wide range of different actors, from scientists and researchers to citizens and the public.
- The increasing tendency towards political steering of scientific research and to implement competitive mechanisms of access to public funds.
- The increasing pressure to obtain faster social and economic benefits out of scientific research by favouring investments in applied research rather than in fundamental research.
- The increasing tendency towards trans-disciplinary research, on one side, and to more specialisation within the different scientific disciplines, on the other.

Another important transformation is the decreasing authority of and people's increasing distrust of science and scientific institutions, which is leading to a growing demand for accountability and public scrutiny of research processes and products, also seen as a way of preventing risks and undesirable impacts.

Similar changes, in the context of the transition to what is termed 'late modernity' (or digital modernity, as David Lyon suggested), are occurring also in other social institutions, such as politics, economics, public administrations, with various forms of diminishing authority and lack of public trust. These include de-standardisation, fragmentation, and increasing social pressure on institutions to become more transparent, effective, productive, and sensitive to societal needs and expectations. Such processes of change are modifying the balance between social structures (including not only institutions, but also social norms, cultural views, behaviours, etc.) and the agency of individuals, that is, the capacity of individuals to more freely think and act as well as to 'build up' their own life, projects, and identity, even challenging the social structures. In late modernity, the agency or the subjectivity of people are weakening social institutions and are producing diversified configurations of social life which are facilitated thanks to other processes such as digitalisation, increasing mobility, and easier access to resources (Archer, 2007; Bauman, 2000; Beck, 1992; Giddens, 1991; Quaranta, 1986).

By and large there is an increasing pressure to close the gap between science and society promoting and deploying scientific and innovation ecosystems that are more open, transparent, and accessible. Science and research are challenged to be more open to citizens, allowing the possibility of public scrutiny of their activities and results (d'Andrea , Marta and only for Part Three Para 2.2. Kahma & Vase, 2017).

As mentioned in the Introduction, this process of change in the internal and external mechanisms of science might also facilitate malpractices or, for our discussion, the design of surveillance technologies, which are risky from a societal point of view, and can produce economic and social costs.

SOCIAL SUBJECTIVITY AND THE EMERGING DEMANDS FOR SECURITY AND AUTONOMY

Considering what we have noted so far, we can say that science and innovation are undergoing a long transitional phase which is characterised at the same time by a weakening of the main social institutions and by an increase in 'social subjectivity'.

With the term 'social subjectivity' we refer to the fact that contemporary societies – due to the processes discussed above – reflect a large-scale increase in the importance, complexity, and density of the cognitive, intellectual and emotional dimensions of individuals. The latter are also characterised by a high degree of uncertainty, since social structures are becoming weaker, more flexible, and more subject to change (Beck, 1992; Giddens, 1991; Quaranta, 1986). We can say that new forms of human agency are emerging, producing a 'surplus' of human energy, so that individuals are more and more 'capable' of generating new ideas, innovating and overcoming everyday life constraints, while their field of action is broader and less limited by territorial boundaries.

The digital ecosystem offers unprecedented opportunities to express such human agency, functioning as a multiplier of the social energy of groups and individuals, in cultural and social life as well as the economy. At the same time, it can jeopardise the identity and the personal security of individuals. Not least, the Internet offers increasing opportunities to criminal actors, both on-line and off-line (Mezzana & Krlic, 2013).

We can thus maintain that there is a connection between the scientific and technological developments and the increased assertiveness of individuals and groups, who can avail themselves of unprecedented opportunities for their expression and potency. The legitimate expectations of citizens to enjoy their rights, including the ability to protect their private sphere, are growing (Cannataci, 2015). Scientific and technological development is deeply interrelated with the widespread awareness of these rights and the possibility of exercising them, but it produces also new risks, while a widespread sense of insecurity increases. The digital revolution, in fact, while improving people's quality of life, offered at the same time, as said, new opportunities for various forms of crime and terrorism, which in turn produced the demand to strengthen security systems through increasingly advanced and intrusive surveillance technologies which themselves produce anxiety about intrusive State control or exploitation from over-the-top private companies.

In such a context, the problem becomes balancing two equally compelling social demands: that of security and that of protection of personal rights, including privacy (Alfonsi, Declich, & Berliri, 2019; Charitidis, Spyrakou, Markakis & Iphofen, 2019; Iphofen, 2014, chapter 5). The question of what is actually

unethical is going beyond well-known issues such as fabrication, falsification, and plagiarism. Referring to surveillance, phenomena such as social profiling through the data science process, or the opacity in the use of advanced technologies for recording and analysing personal behaviour and inclinations challenge all concerned actors to take measures to avoid being involved in practices that could harm the rights of citizens. In fact, misconduct in the field of surveillance can harm not only individual citizens' rights, but can, in a broader perspective, further impair societal trust in science, and in the State and its institutions.

UNDERSTANDINGS OF SURVEILLANCE

To discuss the impact of issues related to surveillance on public trust and social interaction, we should consider how the application of this notion has broadened in recent times. At a first level, we have the more restricted and traditional definition, what can be termed 'State surveillance', that is, focussed on activities carried out by legal entities endowed with a special authority by State institutions and primarily targeted at law enforcement and crime prevention – including terrorism. Nowadays, such activities imply the massive use of digital technologies (smart systems) and the processing of large amounts of data, both collected ad hoc or collected for other purposes. In this view, surveillance activities can be considered as

> any monitoring or observing of persons, listening to their conversations or other activities, or any other collection of data referring to persons regardless whether this is content data or meta data, which is carried out by the State, or in its behalf or at its orders. (Cannataci, 2019)

In this regard, several authors (see for instance Mann & Ferebonk, 2013) point to the fact that the very word 'surveillance', of French origin, implies a 'gaze from above' (*sur veillance*), underscoring the hierarchical and asymmetric relationship between the 'watcher' and the 'watched'.

At the same time, this State activity is presently confronted by the use that organised crime and terrorists are making of new technologies and the Internet (including what is called Deep Internet and Dark Internet) for their criminal activities, off-line and on-line. Thus, law enforcement authorities are also faced with the need to increase their capacity to combat the criminal use and penetration of the new technological environment. Furthermore, in the present context old and new forms of surveillance co-exist, co-support, and feed off each other, thus producing 'mutual augmentation', which could possibly produce much greater and amplified surveillance (Colonnello, Alfonsi, Marta, & Mezzana, 2014; Trottier, 2011). Thus, a relevant area of discussion currently revolves around how to ensure an Internet where the citizens are safe from criminal activities as well as from undue surveillance from law enforcement agencies, while at the same time these same agencies are provided with sufficient capacity to effectively combat the actions of criminals and terrorists. This balance is considered by many to be difficult to strike.

It is important to observe that the deployment of new technologies to some extent challenges the State monopoly on surveillance and opens the way to a

wider range of actors, not only to public authorities. This realisation has brought several authors, including those related to the Surveillance Study Network,[2] to broaden the definition of surveillance from an institutional function to a widespread social practice of which State surveillance is only a special case. Thus, the notion of surveillance society has been introduced, understood as a

> society which functions because of the extensive collection, recording, storage, analysis and application of information on individuals and groups as they go about their lives (big data). In this case private bodies, including big corporations, join the State actors as agents of surveillance for their own purposes, including business. (Surveillance Study Network[3])

This notion implies the need for more diffused and granular use of instruments to check the ways in which the data about personal behaviour are collected and perused. At the same time, the notion of surveillance society focusses on the idea that there are observers (above) and those observed (below) with basically the private sector interacting and competing with the State in *surveilling* the citizens in their private lives.

A further extension in the understanding of surveillance in the contemporary world is achieved by authors like David Lyon, who speaks of a 'Culture of surveillance'. This notion focusses on the agency of citizens/users who are not only passive subjects of surveillance, or merely 'devolve' their personal data, but actively participate in its operation by their daily actions, including surveillance of others (e.g. on social media, see Trottier, 2011), self-surveillance, and 'quantified self' practices (Lupton, 2020). What is to be noted is also the fact that the directionality of surveillance, albeit remaining asymmetrical in power relationships, no longer goes only in one direction, that is, top down, but moves also 'bottom up' (see the notion of 'Sousveillance', i.e. 'watching from below', of Mann, 2013). This means also that some individuals and groups have acquired the capability of recording and monitoring the behaviour of public officials and law enforcement agents, and to some extent of big companies. This multiactor and multilateral surveillance gives rise to various power configurations, both cooperative (e.g. community policing[4]) and confrontational, which challenge the monopoly (now 'oligopoly') of the State and of large corporations on data collection and evaluation. One current example is the case of the death of the American citizen George Floyd, whose last minutes were recorded not only by the police bodycams, and nearby CCTVs, but also by several bystanders, so that the social meaning of the event was from the start framed in a way that highlighted the misbehaviour of the police officials involved. It must be noted that this plurality of visual sources played a significant role also in the legal trial that brought to the conviction of officer Derek Chauvin.

SOCIAL COSTS OF SURVEILLANCE AND SOCIETAL TRUST

As we have discussed, at present surveillance technologies are multiple, ubiquitous, pervasive, heavily relying on ICTs, and are changing fast and becoming

more and more sophisticated so that there is a heated debate about their possible problems, harms, and costs for individuals, groups, and society as a whole. This is by no means a recent development: since the last half of the twentieth century, the ever-increasing use of technology for the discovery and collection of personal information for surveillance and security purposes has raised concerns about risks (e.g. with regard to privacy protection), harms and costs to individuals and groups by social scientists, jurists, ethicists, researchers, and by advocacy and citizens' organisations. Surveillance studies provided interesting categories to analyse the application of such technologies in order to identify the main issues to be taken into account (Lyon, 2007; Marx, 2002; Macnish, 2018). Based on a review of the relevant literature, we provide here a quick overview of the social costs that can derive from the use of contentious, inappropriate, or non-proportionate practices. As a preliminary observation, we can note that privacy protection is always at the centre of concern, in the reflection about surveillance activities. Also in this case there are different definitions of privacy and personal data protection (from the right to be let alone, to privacy as a fundamental right of identity protection and self-determination and freedom of expression). For our purposes, we define privacy as a dynamic social form of defence of the self and of its subjectivity, at various levels: from the ethological level, linked to the defence of one's own personal territory, to the psychological level, and gradually up to the legal level (Mezzana & Krlic, 2013). On the basis of the relevant literature, it is possible to identify three areas of concern about the social costs of surveillance. For identifying these areas, we used the findings of the EU Project RESPECT (Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies) contained in the 'Final report on social costs of surveillance' (Colonnello et al., 2014).

A first area of concern is related to the use and management of data (Big data and personal data) and data processing technologies (including smart and automated ones). This area includes:

- Social sorting, that is, social classification and selection for valuative purposes of individuals and groups often based on not accessible/transparent criteria (often biased by stereotypes – categorical suspicion related to gender, ethnic, racial, religious, or political aspects) incorporated in algorithms and in automated technologies (e.g. in the case of CCTV it can contribute to the construction and reinforcement of a condemnatory gaze on the powerless).
- Surveillance/function creep, that is, the interchangeability of digital technologies, or in other words the gradual widening of the use of a technology or system beyond the purpose for which it was originally developed to other uses and ends; or data collected for one purpose being used for another.
- Data slippage, that is, moving of data from one context to another.
- False positives, exposing people to the harm that can arise from errors or misidentification or misinterpretation of data or behaviours recorded.
- Leaky containers, namely the practices by which, with the development of new technologies and greater national and global interconnections, there is a

> 'loss' (intentional or accidental) of personal information from one system to another, which may damage the reputation of another person, causing harm to their private, social, and economic life, undermining their credibility within a social group or community.

This area includes also the important ethical issue of dual use, defined as the fact that a product or a technology can be used with both good and bad intentions/aims (bad intentions that have to be considered among the case of malpractices, like e.g. deliberate or accidental releases of private information – data breach). In the case of surveillance technologies, dual use is a very relevant topic, which involves using crime prevention technologies like phone interception, face recognition in social media, or cryptography, for political uses against dissidents or minority groups, with a violation of human rights. Part of the current debate veers on the necessity and possibility to incorporate remedies for such concerns in the very design and deployment of surveillance technologies.

A second area of concern focusses on the social costs related to the deployment and use of inappropriate or non-proportionate surveillance technologies and activities on individuals and groups. As we said before, privacy is important for protecting the identity and the subjectivity of individuals. Inappropriate or non-proportionate surveillance activities might produce effects and harms on personal identity (defined as the capacity of individuals to control the reality in which they operate), on autonomy (defined as decision making power and freedom of movement and action) and on the reputation (defined as the protection of the good names of people). In this context, the possible common harms identified include exclusion and discrimination; stigmatisation of groups and lifestyles; constraints to mobility; stalking and harassment; limitation and self-censorship; change in social behaviour (e.g. in public space for the presence of CCTV, or public shaming in social media); loss of opportunities in one's private, social and professional life; loss of personal/group social capital and relations. In this context, particular attention has to be devoted to gender-based discrimination and to the stigmatisation of persons with disabilities, indigenous people, or migrants (Cannataci, 2018, 2019).

A third area concerns, in a broader perspective, the effects that inappropriate and non-proportionate surveillance practices, even if enacted in the name of security, produce in further diminishing social and public trust and confidence in government, public institutions, and private organisations, including the de-legitimisation of the police in their role and on how this role is performed. Furthermore, such surveillance activities, in some cases, might affect also the quality of democracy and the full participation in the social, political, and economic life of individuals and groups, with phenomena such as abuse of power in the name of national security and protection from terrorism, suppression, or inhibition of political dissidence, reduction of fundamental civil liberties and fundamental rights, or forms of mass espionage/surveillance. Furthermore, some bad practices of surveillance like categorical suspicion, judicial errors, manipulation of evidence, or miscarriage of justice (tied with the use of biometric surveillance) might also affect the virtuous operation of the administration of justice.

Finally, beyond the deployment of *sousveillance* activities by citizens that we discussed earlier, the surveillance technologies can produce, as a reaction, also phenomena of resistances and non-compliance performed by individuals and groups using different forms and tools.

At this point of our reflection, the question is how to design and deploy responsible, appropriate, and proportionate surveillance technologies and activities able to cope with both the demand for security and autonomy, and to the new challenges posed by the new frontiers of surveillance technologies.

TOWARDS RESPONSIBLE SURVEILLANCE

From what we have discussed so far, it does appear that surveillance and its culture are a fundamental feature of contemporary societies. In fact, surveillance activities in the different definitions that we have presented are becoming more and more pervasive and granular, by means of increasingly diversified and advanced technologies. At the same time, however, their deployment has become multilateral not only because State actors are interacting/competing with private actors but also because citizens individually and as organised groups can play an active role and, at certain conditions, reverse the 'gaze' from the bottom up. This gives rise to several overall power configurations that, albeit asymmetrical in terms of potency, are by no means exclusively top down. These new configurations can include also horizontal relationships such as peer-to-peer surveillance or self-surveillance.

Thus, the context of surveillance can be seen as closely connected to those forms of enhanced social subjectivity that we have discussed above and represents also a major challenge, in that the many layered issues that it poses, including the risks and social costs discussed in the previous paragraph, are not yet fully socialised, or, we might say, are 'under-socialised'. By this we mean that security and surveillance technologies, strategies, and arrangements are being developed at a very fast pace so that their embeddedness in society is still weak, developed with scant interaction with the different stakeholders and with insufficient public control and assessment of their impacts, including considerable heterogeneity in the evaluation instruments. This lack of socialisation is at the origin of economic and social costs to individuals, groups, and societies, also due to the implementation of questionable practices of surveillance. Furthermore, this occurs in a context in which societies and citizens are much more reactive and attentive with respect of malpractice and this might reinforce distrust in science and research, and in institutions. On the contrary, what we mean by socialisation is the capacity to adapt technologies to the needs, expectations, and problems of society and the capacity to control social dynamics incorporated in science and technology. This socialisation of science, technology, and research is not to be regarded as a unitary and linear process, but a composite and multidirectional one, requiring the involvement of actors and groups (Bijker & d'Andrea, 2009; d'Andrea, Quaranta, & Quinti, 2005; Mezzana Ed., 2011).

To sum up, what seems to be lacking is a shared awareness of what is at stake and of viable ways to exercise social responsibility in view of inclusive and multilateral forms of governance, in line with what authors like David Lyon have called 'digital citizenship'.

A possible path towards a full socialisation of surveillance could perhaps be traced by looking at the perspective of Responsible Research and Innovation (RRI) launched by the European Commission to manage science–society relations in the European Research Area (Burget, Bardone, & Pedaste, 2017; European Commission, 2012; Owen et al., 2013; van den Hoven, 2014; Von Schomberg, 2011, 2019). To be sure, currently there is a widespread debate on the merits of the RRI approach, that is, questioning its very definition and purpose. In our understanding, RRI can be viewed as a policy reaction to the changes already occurring in science and innovation or, better, an attempt to drive these changes towards desirable or at least manageable outputs.

In this regard, RRI can be considered as an umbrella concept, that is supposed to advocate an action to better embed science, research, and innovation in the fabric of society, by pointing to certain key elements of concern such as: gender equality in science, open access to research data and publications, research ethics and integrity, citizen engagement, science education, and governance. These key elements are often integrated by four dimensions: inclusiveness, anticipation, responsiveness, and reflexivity, which might be relevant in the context of surveillance (Compass, 2018; Floridi, 2012; Klimburg-Witjes & Huettenrauch, 2021; Kormeling, 2018; Menevidis, Mohd Nor, Briege and Mitrou, 2014; Stahl, 2013; SIENNA, 2020; Van de Poel et al., 2020).

Inclusiveness seems in fact to respond to the multilateral feature of present-day surveillance. This requires that all actors and stakeholders involved (State agencies, technologists, scientists, companies, policymakers, citizens, civil society organisations, etc.) are able to interact with each other. To fully satisfy the condition of inclusiveness, appropriate means need to be devised to allow citizens to voice their perspectives and concerns about the deployment of surveillance technologies in everyday life situations. At the same time, the anticipatory dimension is of paramount importance in a field where a fast-paced technological development constantly produces new technical possibilities that in turn call for ethical decisions, social acceptance, and normative frameworks. Furthermore, the pace at which technological developments tend to happen requires the capacity for timely responses to the challenges of a constantly changing landscape. Finally, as we pointed out already, what is also required is the attitude of all concerned actors to be able to reflect on the implications of such developments in order to build a shared vision of what is at stake in order to cope with an environment in which surveillance with its contribution to public security and with its risks and drawbacks is so much intertwined in the fabric of contemporary social life.

In conclusion, it is necessary to understand the conditions by which emerging social subjectivity can be informed by what has been termed an 'ethics of care' in order to assure fundamental instances of fairness, data justice, visibility, and recognition in the design, deployment, and use of surveillance technologies.

NOTES

1. These include CCTV, RFID, SMART technologies, geo-localisation technologies, biometric technologies, voice identification, face recognition, Data science and Big Data, Artificial intelligence, ICTs, Internet of things, wearable technologies, encryption and anonymisation technologies, use of malicious malware and spyware, social media scan, etc.
2. *Surveillance Studies Network* (https://www.surveillance-studies.net/) is a charitable company registered in UK, but international in its membership, dedicated to the study of surveillance in all its forms. They publish the peer reviewed journal *Surveillance and Society* (http://surveillance-and-society.org/) and acts as a clearing house for social science and policy research and consultancy about surveillance.
3. This is the definition provided by the Surveillance Study Network, in its blog post 'An introduction to the surveillance society', available at https://www.surveillance-studies.net/?page_id=119.
4. See Mifsud Bonnici and Cannataci (2018).

REFERENCES

Alfonsi, A., Declich, G., & Berliri, M. (2019). Surveillance, privacy and covert research: Current challenges to the research ethics and integrity. In *PRO-RES workshop on covert research, privacy and surveillance* (PRO-RES PROmoting integrity in the use of RESearch results), Rome, April 11, 2019.

Archer, M. S. (2007). *Making our way through the world: Human reflexivity and social mobility*. Cambridge: Cambridge University Press.

Bauman, Z. (2000). *Liquid society*. Cambridge: Polity Press.

Beck, U. (1992). *Risk society: Towards a new modernity* (Vol. 17). London: Sage.

Bijker, W., & d'Andrea, L. (Eds.). (2009). *Handbook on the socialisation of scientific and technological research (Social Sciences and European Research Capacities (SS-ERC) Project)*. Rome: European Commission.

Burget, M., Bardone, E., & Pedaste, M. (2017). Definitions and conceptual dimensions of responsible research and innovation: A literature review. *Science and Engineering Ethics*, *23*(1), 1–19.

Cannataci, J. (Ed.). (2015). *The individual and privacy. The library of essays on law and privacy* (Vol. 1). New York, NY: Routledge.

Cannataci, J. (2018). *Right to privacy. Report of the special rapporteur on the right to privacy*. General Assembly, Human Rights Council, Fortieth Session, 26 February–23 March 2018.

Cannataci, J. (2019). *Right to privacy. Report of the special rapporteur on the right to privacy*. General Assembly, Human Right Council, Fortieth Session, 25 February–22 March 2019.

Charitidis, C., Spyrakou, E., Markakis, V., with the contribution of Iphofen, R. (2019). Thematic priorities report D2.1. PRO-RES D2.2. PRO-RES PROmoting ethics and integrity in non medical RESearch.

Compass. (2018) Responsible innovation roadmap cyber security. Retrieved from https://innovation-compass.eu/roadmaps/roadmaps/ri-labs-cyber-security/

Colonnello, C., Alfonsi, A., Marta, F. L., & Mezzana, D. (2014). Final report on social costs of surveillance. RESPECT (Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies) Deliverable D13.4.

d'Andrea, L., Quaranta, G., & Quinti, G. (2005). *Manuale sui processi di socializzazione della ricerca scientifica e tecnologica*. Rome: CERFE.

d'Andrea L., Marta, F. L., and only for Part Three Para 2.2. (2017). *FIT4RRI D1.1 – Report on the literature review*. doi:10.5281/zenodo.1434349

d'Andrea, L. (2019). *State-of-the-art review of documented experiences – Document 6 – Approaches to RRI*. GRACE – Grounding RRI Actions to Achieve Institutional Change in European Research Funding and Performing Organisations. Knowledge & Innovation Srls.

European Commission. (2012). *Responsible research and innovation. Europe's ability to respond to societal challenges*. Luxembourg: Publication Offices of the European Union.

Etzkowitz, H., & Leydesdorff, L. (2000). The dynamics of innovation: From national systems and "mode 2" to a triple helix of university–industry–government relations. *Research Policy*, *29*(2), 109–123.

Floridi, L. (Ed.), (2012). *The Cambridge handbook of information and computer ethics*. Cambridge: Cambridge University Press.

Gibbons, M., Limoges, C., Nowotny, H., Schwartzman, S., Scott, P., & Trow, M. (1994). *The new production of knowledge: The dynamics of science and research in contemporary societies*. London: Sage.

Giddens, A. (1991). *Modernity and self-identity: Self and society in the late modern age*. Palo Alto, CA: Stanford University Press.

Iphofen, R. (2014). Ethical issues in surveillance and privacy. In A. W. Stedmon and G. Lawson (Eds.), *Hostile intent and counter-terrorism: Human factors theory and application*. 59–72. Aldershot: Ashgate.

Klimburg-Witjes, N., & Huettenrauch, F. C. (2021). Contextualizing security innovation: Responsible research at the smart border?. *Science and Engineering Ethics*. doi.org/10.1007/s11948-021-00292-y

Kormeling, G. (2018). *Responsible innovation, ethics, safety and technology. How to deal with risks and ethical questions raised by the development of new technologies* (2nd ed.). Delft: TU Delft Open.

Leydesdorff, L., & Etzkowitz, H. (1998). The triple helix as a model for innovation studies. *Science and Public Policy*, *25*(3), 195–203.

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

Lyon, D. (2018). *The culture of surveillance. Watching as a way of life*. Cambridge: Polity Press.

Lupton, D. (2020). *Data selves. More-than-human perspectives*. Cambridge: Polity Press.

Macnish, K. (2018). *The ethics of surveillance. An introduction*. New York, NY: Routledge.

Mann, S. (2013). The inevitability of the transition from surveillance-society to a veillance-society: Moral and economic grounding for sousveillance. In *2013 IEEE international symposium on technology and society (ISTAS)*. 18–34. 27–29 June 2013, University of Toronto, Toronto, Canada.

Mann, S., & Ferebonk, J. (2013). New media and the power of politics of sousveillance in a surveillance-dominated world. *Surveillance and Society*, *11*(1/2), 18–34.

Marx, G. T. (2002). What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance & Society*, *1*(1), 9–29.

Mezzana, D. (Ed.). (2011). *Technological responsibility. Guidelines for a shared governance of the processes of socialization of scientific research and innovation, within an interconnected world, SET-DEV, 7th Framework Programme for Technological Research and Development of the European Commission*. Rome: Consiglio Nazionale delle Ricerche.

Mezzana, D., & Krlic, M. (2013). The current context of surveillance: An overview of some emerging phenomena and policies. *European Journal of Law and Technology*, *4*(2). https://ejlt.org/index.php/ejlt/article/view/187/380

Mifsud Bonnici, J. P., & Cannataci, J. (Eds.). (2018). *Changing communities, changing policing*. Graz: NWV.

Menevidis, Z., Mohd Nor, R., Briege, C. & Mitrou, L. (2014). Responsibility. *D6.2. Policy brief: RRI for security*. doi.10.13140/2.1.2996.3846

Nowotny, H., Scott, P., & Gibbons, M. (2001). *Rethinking science: Knowledge and the public in the age of uncertainty*. Cambridge: Polity Press.

Owen, R., Stilgoe, J., Macnaghten, P., Gorman, M., Fisher, E., & Guston, D. H. (2013). Framework for responsible innovation. In R. Owen, M. Heintz, & J. Bessant (Eds.), *Responsible innovation*. 27–50. Chichester: Wiley.

Quaranta, G. (1986). *L'era dello sviluppo*. Milano: Franco Angeli.

SIENNA. (2020). *Project policy brief #1. Enhancing EU legal frameworks for AI & robotics*. Zenodo. http://doi.org/10.5281/zenodo.4332661

Stahl, B. C. (2013) Responsible research and innovation: The role of privacy in an emerging framework. *Science and Public Policy*, *40*(6), 708–716.

Trottier, D. (2011) *Mutual augmentation of surveillance practices on social media*. Kingston: Queen's University.

Van de Poel, I., Asveld, L., Flipse, S., Klaassen, P., Kwee, Z., Maia, M., … Yaghmaei, E. (2020). Learning to do responsible innovation in industry: Six lessons. *Journal of Responsible Innovation*, *7*(3), 697–707.

van den Hoven, J. (2014). *Responsible innovation in brief*. Delft: The Delft University of Technology.

Von Schomberg, R. (Ed.). (2011). Towards responsible research and innovation in the information and communication technologies and security technologies fields. A report from the European Commission Services. doi.10.2777/58723

Von Schomberg, R. (2019). Why responsible innovation. In R. Von Schomberg & J. Hankins (Eds.), *The international handbook on responsible innovation. A global resource*. 12–32. Cheltenham and Northampton: Edward Elgar Publishing doi:10.4337/9781784718862

Ziman, J. (2000). *Real science. What it is, and what it means*. Cambridge: Cambridge University Press.