

Chapter 6

Engaging Small and Medium-Sized Enterprises in Responsible Innovation



Catherine Flick, Malcolm Fisk, and George Ogoh

Abstract A significant part of responsible innovation is engagement with diverse groups of stakeholders; this remains true for projects investigating responsible innovation practices. This chapter discusses strategies for engaging small and medium-sized enterprises (SMEs) in co-creating visions of and plans for implementing responsible innovation, drawing on the example of engagement with United Kingdom cyber security companies. The key aspect of the engagement was building trust between the responsible innovation researchers and the companies. Trust was built by a movement away from traditional recruitment procedures for research projects, towards proactive engagement with the culture and traditions of the sector – participating in company sponsored talks and conferences, finding ways to communicate effectively, and ensuring a tailored message that fit the expectations and requirements of the sector. This chapter reviews the context in which the recruitment took place, the assumptions made prior to recruitment, the approaches taken, the revisions made to these approaches, and ultimately offers some general recommendations for industry engagement in responsible innovation activities.

Keywords Cyber security · Responsible innovation · Engagement · Small-medium enterprises · Trust

6.1 Introduction

Some of the most significant challenges for responsible innovation in industry include raising awareness of the concept, showing businesses its value, and capturing businesses' interest in implementing responsible innovation in their own research and development practice. This chapter looks at the engagement of cyber security SMEs (small and medium-sized enterprises) in responsible innovation, by

C. Flick (✉) · M. Fisk · G. Ogoh
School of Computer Science and Informatics, De Montfort University, Leicester, UK
e-mail: cflick@dmu.ac.uk; malcolm.fisk@dmu.ac.uk; george.ogoh@dmu.ac.uk

investigating the techniques that were used to recruit companies for a series of online and face-to-face peer co-creative workshops on implementing responsible innovation within the United Kingdom cyber security sector. The analysis of these engagement methods culminates in a set of general requirements and recommendations for engaging primarily with cyber security companies, but which also have general relevance to other industry sectors.

Responsible innovation, as has been seen in previous chapters, is a set of practices by which researchers and innovators engage with society to identify social and ethical impacts and issues of the technologies they are developing. Largely referred to in the academic world as the more cumbersome “responsible research and innovation” (RRI), definitions of responsible innovation are many and varied, but the general idea is that innovation should include society, deliberate on ethical and social issues, and align with societal needs (European Commission and Directorate-General for Research and Innovation 2013; Owen et al. 2013; Von Schomberg 2013). However, the concept of RRI does not have much penetration into industry (Stahl et al. 2017), and industry players are more likely to know and recognise terms such as corporate social responsibility (CSR) (European Commission 2011) or more simply, business ethics. To reflect this finding, and for reasons we discuss below, we henceforth refer to RRI as “responsible innovation” (RI).

In order to engage effectively with cyber security companies on topics surrounding RI and engage them in the planned workshops, a communications strategy needed to be devised. The approaches that were successful focused on the opportunities available to SMEs, were individually tailored to their spaces and requirements, and helped to ensure that the SMEs were comfortable in discussing confidential information. These experiences found that a desire for the development of trust with the general public, consumers of companies’ products and services, and/or other businesses was a major driving factor in their engagement with RI.

This chapter reviews the context in which the recruitment of the companies took place, the assumptions made prior to recruitment, the recruitment approaches taken, the revisions made to these approaches, and offers some general recommendations for industry engagement. It argues that one of the most effective strategies for recruitment and engagement of SMEs is to become involved in the existing communication spaces of the sector, rather than expecting companies to respond to calls for interest.

6.2 Responsible Innovation for Cyber Security Companies

Previous chapters have explored the potential benefits of following a value-based approach to corporate innovation. However, the value propositions need to be well-defined and to generally align with existing goals within the company if they are to be considered useful. For example, for cyber security, trust seems to be a significant factor in interest in RI. The value that public and customer trust has for each cyber security company is significant, although this might not initially have been seen by

cyber security SMEs in monetary terms and business sustainability. However, when RI activities were explained to cyber security SMEs in the context of ethics, responsibility, privacy, and trust, and with only a passing mention of ‘responsible innovation’ (instead of attempting to define RI explicitly), companies could see the alignment with their existing value statements, medium-long term goals, and discussions that had already taken place internally (especially regarding ethics). In fact, for cyber security companies, ethics and trust are regular topics of industry discussion, with philosophical differences arising between different camps on particular ethical dilemmas, such as disclosure of vulnerabilities (responsible disclosure vs. full disclosure), and bug bounties (rewards offered by companies for finding exploitable bugs in their software) (Hughes 2015; Lefkowitz 2017).

The emphasis on security is growing in a more uncertain and technologically-dependent world. Cyber security is therefore a natural growth area for industry, and a good example subsector of the more general IT industry, much of which grapples with uncertainty. It is a loosely defined sector encompassing many different types of security-related products and services. Much of the cyber security market is business-to-business, offering reputation protection, security of data, forensics and fraud detection, and server security. However, cyber security companies are also responsible for products and services that consumers use, such as security cameras, identity management apps, encryption of devices, and educational materials. The nature of cyber security’s past can be suggestive of a somewhat ‘cowboy’ culture, with its frontiers of technological crime prevention often seen as a ‘grey area’ - including ‘white-hat’ (those who operate within legal and ethical norms), ‘grey-hat’ (those who operate mainly in a legal sphere, but occasionally exploit opportunities of policy vacuums, usually within ethical norms), and ‘black-hat’ hackers (those who break legal and ethical norms) operating on both sides of the law to meet their goals. Coupled with the complexity of the topic and issues, as well as poor representation of the field in movies and TV shows, there is a significant lack of understanding of what cyber security is, what its goals are, and how it works. This can translate into a lack of trust between end-users and security companies and their products, or to a view of cyber security products and services as ‘grudge purchases’ made by companies who view the sector much as they see insurance.

Thus, the value of RI to cyber security companies is in helping them to develop these trust relationships with their clients, whether they are individual end-users or companies. In this way, a company can show its trustworthiness to users who may not understand the technicalities, theoretical aspects, or even the user interfaces for cyber security. And in helping the cyber security sector to engage in openness, transparency, ethics and responsibility, along with other RI practices, clients who do not understand the inner workings of the technologies involved can develop a stronger trust relationship with the company.

We found in our work that companies are eager to engage with the concept of trust. The strategies detailed in the following section point to ways of harnessing companies’ interest.

6.3 Recruitment Aims and Strategies

This section looks briefly at the aims of the RI research to provide context, then in more depth at the strategies which were chosen to approach the cyber security community to participate in the project, and describes the most effective engagement processes. It also discusses complications that arose after companies had made a commitment to the process. The resulting approach was effective in engaging companies for the RI workshops and helped build a significant rapport with the companies that, in turn, improved the outcomes of the workshops.

The aim of these interventions was to engage companies in a series of on- and off-line workshops. It was envisaged that the companies would work together to develop a ‘responsible innovation roadmap’ co-creatively with their peers, facilitated by the workshop leaders. Initially, there were to be three webinar-style online workshops, and two face-to-face workshops, where the companies would come together to co-create the shared roadmap using foresight and backcasting methodologies.¹ The cyber security companies were to be from the UK and considered as SMEs (up to 250 employees). SMEs were targeted as approximately 50% of SMEs in the UK are engaged in innovation activities (Department for Business, Energy, and Industrial Strategy 2017), but unlike large companies, they often do not have significant corporate social responsibility (or similar) arms.

Prior to the strategy being developed by which SMEs would be approached, however, a concern arose that cyber security companies might be more difficult to engage than other sectors due to their more secretive nature, particularly if this was to be in a peer-led co-creative exercise such as the planned workshops. This concern was based on discussions with cyber security experts within academia about company involvement with their research, but, as this article will show, the concerns were relatively unfounded, as the topics of ethics, trust, and other technical philosophical discussions were seen by the companies *individually* to be interesting and relevant. However, it took some time to realise this specific entry point for engaging with companies, as is explained below. The peer-led co-creative exercise however, was correctly identified to be a problematic approach for this sector, regardless of interest in the topics. The evolution of the planned co-creative exercises is also detailed below.²

Firstly, a generic, academic-style call for participation was developed. This was sent to a number of contacts identified by members of the research project. Some effort was made to circulate this call through established cyber security fora, for example, the UK Cyber Security Forum, as well as more personal networks, such as university cyber security partners. This was based on the assumption that companies would be most likely to respond to personal contacts and through advertisements on an industry website.

¹ More information on the workshop methodology and approaches can be found in D2.5 at <https://innovation-compass.eu/deliverables-2/>

² Examples of the drafts discussed below are available from the authors by request; due to space limitations we have included only the final, successful, recruitment letter in [Appendix](#).

After poor engagement with this method (i.e. none), discussions with several cyber security experts were undertaken (university researchers with industry contacts; cyber security experts from other countries). Advice was taken on the nature of the ‘sales pitch’ (i.e. the description of the activities and the benefits to the companies in taking part) to make it more focused on the benefits that companies might gain from participating, as well as to avoid the implication that this would be largely an academic activity that might berate companies for unethical behaviour. The ‘RRI’ terminology was removed at this stage as it was considered by our advisors to be jargon, and could result in restricted discussion to the constituent parts, such as ethics. A more conversational tone was adopted, addressing some of the companies’ potential concerns; avoiding what might be seen as any moralising attitude or the pursuit of impractical theoretical outputs from academics; and included clear reference to links with established business organisations that were partners in the project.

With this new pitch greater interest in the project was generated, but no companies confirmed any commitment to engagement. It seemed there was still some confusion as to what the benefits of participating in the research were and what was required of the companies, especially in terms of the time commitment. Significant discussion at a project meeting came up with the idea of pitching the workshops as free ‘innovation consulting’ to see if that would impact the involvement of companies. In this rather lengthy pitch, it was possible to demonstrate knowledge of the issues cyber security companies faced.

Unfortunately, this new pitch did not work very well either, perhaps because of its length (six paragraphs and some bullet points), or perhaps because it seemed a bit too good to be true (in fact, one of the participant companies regularly checked to make sure they didn’t have to pay for anything). Also, it seemed that the relatively lengthy time commitments envisaged (“less than a day and a half spread over a couple of months”) were considered particularly onerous, and the collaborative working was seen as too complicated, in part due to the intellectual property that could be compromised if collaborative activities were undertaken. Further discussions within the project offered a revised and final ([Appendix](#)) research protocol, with two 2–2.5 h face-to-face workshops in which the researchers came to the companies. A revised sales pitch concentrated on the potential benefits for the companies from engaging in the activities, focusing on topics such as trust-building and ethics.

Another change in strategy was to become engaged in activities that the companies were running themselves. In this way, rather than asking companies to come into what they might perceive as an academic world somewhat detached from commerce; the academics would be working in the world of industry. This was complemented by engaging in talks and networking events (De Montfort University Cyber Forum, IOActive’s HACK::SOHO, Malvern and South Wales Cyber Security clusters seminar sessions and workshops, a company launch) and speaking at industry venues. The ability to engage with the audience on the topics of ethics, responsibility and trust helped to validate the expertise of the researchers and the development of trust relationships with company representatives. For some companies, knowing that others had already taken up the offer also helped establish this trust relationship

with project engagement and workshops taking place, sometimes reinforced through recommendations from their advisory boards.

Personal connections made through face-to-face discussions at networking events or talks also made a significant difference to the uptake of our subsequent workshops, compared with email introductions, and even more than cold-emailing. Frequently, the companies pointed to a specific set of issues they wished to be discussed in workshops, either problems they had encountered that we might give tailored advice on, or asking us to help them consider different options available to them as they moved from being a very small company of only a few employees to a more structured and larger company. Once again, the focus was around how the companies would benefit. They did not want to generally contribute to research without a well-thought-out set of benefits that they would receive in the process. Additionally (again reinforcing the importance of the interpersonal relationships) being able to show expertise in the specific area of cyber security (i.e. being able to 'talk shop') had a definite advantage in terms of showing trustworthiness and the relevance of the RI activities the companies were being asked to participate in.

Once the companies had taken up the offer, and the initial workshops were set up, some interesting issues around informed consent forms emerged. Discussing confidential business information is relatively taboo in cyber security as these companies are by nature generally quite secretive. It was necessary, therefore, to reinforce the initial trust that had been established through e.g. the use of appropriate consent forms, signing non-disclosure agreements, and other mechanisms. The informed consent procedures followed a fairly standard approach that is typical for university-led research – ensuring that participants understand what the research is about, what information will be taken, how the information can be used, and how they can withdraw from the study. For the workshops, the written work the participants developed and the discussions that were recorded (video or audio) were the main pieces of information taken from the experience.

Usually, for this sort of research, these procedures are easy to gain ethical approval for. This project was no different, and ethical approval was gained from the De Montfort University Ethics Review Board for the Faculty of Technology. However, the companies participating in the workshops, often with their legal advisors present, had difficulty with the (UK academic standard) consent documents. One company had issues with the representativeness of the discussion – with the employees in question being subject to non-disclosure agreements about company procedures and otherwise not speak for the company. Related issues were: How could they engage in this sort of research where they are being asked to discuss company approaches to responsible innovation? Were they speaking personally, or representing the company? After the CEO reassured the employees that they would not be breaking their contracts to discuss anything he or she was open to, the workshop continued. Another company asked that the researchers should also sign non-disclosure agreements about the specific company processes and procedures that might be discussed although all of these conditions were covered by the informed







consent form and research ethics approval underpinning the research. Clearly the companies felt they needed an added level of security for their intellectual property. There was, furthermore, a seeming parallel between the lack of understanding of how university research projects function and the relationships between cyber security companies and end-users or clients (as previously discussed) who often don't understand how the cyber security technologies work.

With trust in the research process having been reaffirmed, the companies were prepared to trust the researchers with significant amounts of useful information to further understand the opportunities, challenges, costs and barriers to implementing RI practices in their businesses. This allowed unparalleled access to their processes and gave emphasis to the need for trust in the research process. Having succeeded in establishing such trust with four cyber security SMEs, a total of eight workshops took place.

6.4 Discussion

The lessons from the approaches discussed above are important in the context of recruiting and engaging with companies for academic research around RI. These may be generalisable and any recruitment strategy could adapt these lessons to their own specific industry sector. The lessons are illustrated in Table 6.1 and discussed below.

Table 6.1 Summary of findings

		
<p>Coming down from the ivory tower</p>	<p>Standard ethical approaches may not be recognised</p>	<p>The need for expertise</p>
		
<p>Tailoring</p>	<p>Failure of standard academic approaches</p>	<p>One-to-one instead of one-to-many</p>

6.4.1 The Importance of Coming Down from the Ivory Tower

One of the key lessons was that small companies in particular do not often have the resources to engage with research if it involves them coming to the researchers. More importantly, in going to the activities that the companies themselves initiated, a signal was sent that the researchers a) understood both their space, and that they had these activities in the first place; and b) were happy to engage on their terms (including accommodating and facilitating discussion on topics of particular concern to them). This helped to establish the element of trust whereby the companies would ‘host’ (food and refreshment and meeting venue) as well as engage with the researchers on a reciprocal basis.

6.4.2 Standard Ethical Approaches May Not Be Recognised

One of the more surprising lessons was the pointer to how much academic researchers may trust in ethical procedures and research ethics committee approvals granted for these sorts of activities. The fact that some of the companies required additional layers of protection for their intellectual property and procedural approaches was particularly interesting considering that they were, in fact, covered by the ethical approval processes. Is this a sign that there is little trust propensity for scientific research ethics processes outside of academia? Or is it more indicative of the particularly secretive natures of cyber security companies? No other sector companies engaged in our project had issues with the consent documentation, but perhaps this is because those other sectors addressed in the project (biomedicine and nanotechnology) are more closely aligned with traditional academic scientific research, where there is familiarity with and trust in these procedures.

It is important that this issue is considered by researchers when engaging with companies, and certainly those in the cyber security sector. It follows that the ability of companies to sign non-disclosure agreements that cover the same conditions as more standard academic consent procedures should be discussed with university legal services and ethics review committees, and legal teams within companies given time to investigate them. Additionally, fall-back options should be considered. For one company, for instance, workshops were only recorded audio, as video recording was considered too invasive.

6.4.3 The Need for Expertise in the Target Area

Throughout this whole procedure, the need for the researchers to ‘prove themselves’ as experts with reasonable knowledge in the specific sector area, and not just in applied ethics/responsible innovation was clearly important. A significant

understanding of technical issues was definitely advantageous when working with the companies. Being able to tailor questions to help each company delve into the ethical questions surrounding their specific lines of work was very helpful to get detailed, in depth, responses. Cyber security is a widely varied sector, and with expertise of many of the different areas it is clearly easier for the researcher to establish trustworthiness, and more likely that the company will have a trust propensity for the researchers. Indeed, the company's understanding must be that the researchers will understand some of the complexities of the sector and their business and, therefore, be able to use the research outcomes effectively.

Similarly, the use of "known experts" as part of the pitch, particularly those in cyber security companies' areas of interest, including the in-house expertise of cyber security researchers at the university, the local police, business support organisations, and others, improved the credentials of the research team, showing that we were engaged with other organisations and businesses outside of the university.

6.4.4 Tailoring Is Advantageous

Expertise in the subject area can also help to fulfil another requirement, that of tailoring the discussions to the specific company. The cyber security workshops were characterised by co-creation activity by peers and were conducted with several members of the same company. This allowed for tailoring of the information provided to the company, rather than a more generic approach. Such tailoring requires more understanding of the company involved, and expertise on the part of the researchers to be able to analyse and report back on the results. By following this approach, the results from the cyber security workshops allowed a richer set of outcomes than those which arose from the 'collective' approach to workshops that were undertaken for the biomedicine and nanotechnology sectors elsewhere in the project.

6.4.5 The Failure of Standard Academic Approaches

Standard academic approaches for research recruitment generally include calls for participation via email lists, or newsletters, or other methods that are often picked up by multipliers. These kinds of 'passive consumption' requests for engagement were largely unsuccessful in this study. Unlike with academic calls for papers or similar, these kinds of activities are not part of the day-to-day business of cyber security companies, which may explain why such calls were regularly ignored. Other standard academic approaches to potential participants, such as offering to pay for travel and accommodation, food, etc., also did not work. This may be explained by the fact that many of the SMEs engaged with were time-poor, with several potential participants dropping-out of the process due to lack of time or the

inability to agree a mutually convenient time. Clearly to contribute a day or two of their time is overly burdensome for many SMEs, even with financial compensation. The fact that the researchers were willing to travel to the companies was well-received by the companies involved, as was the reduction of the time investment required.

6.4.6 One-to-One Instead of One-to-Many

Finally, the advantages of sending personalised, follow-up emails after a personal introduction or meeting at a networking or talk event are significant. As has been noted, the original approaches of sending information to potentially interested parties via multipliers (e.g. the university's cyber security network, the UK cyber security forum, and larger multipliers such as more general business networks) were largely unsuccessful. Large-scale advertising allows for relative anonymity and, it is suggested, can lead to a lack of response. Ignoring *personal* emails after initial connections are made is much less socially acceptable and, even when invitations are declined, these refusals can offer useful insights into the reasons (e.g. time constraints, concerns about confidentiality). Additionally, recommendations from boards of trustees/advisory boards for their companies to participate, as well as their having knowledge that other well-respected companies are participating, helps increase the predisposition to take part. The trust companies have in advice from these boards also contributes to the overall trust propensity of the cyber security practitioners in the researchers themselves.

6.5 Conclusion and Recommendations

These experiences describe how hard it sometimes is to recruit companies to work with RI research projects. Often there are conflicting ideas of roles, benefits, what is required, and what outputs are created. In moving from an academic sphere to a business sphere, going into their world and becoming involved in their events, approaches, and ultimately understanding their positions, it was possible to recruit companies who not only initially engaged, but over time became longer-term partners with the project, offering to go above and beyond the minimal engagement requirements. These interactions point to a high level of trust between the researchers and the companies: not just that the researchers were trusted, but that they were trustworthy. This reflects, it is considered, the desire that the companies have to, themselves, be seen as trustworthy beyond the cyber security sector: pointing to such "trust" being a key reason for engaging with the activities during the work-

shops. This validates the usefulness of locating a key value that the industry is likely to engage with, and that aligns with RI principles and practices, in order to use it as a method for engagement.

Overall, the following approaches worked best for engaging with cyber security companies about RI:

- Removing the academic terminology of “responsible research and innovation” as a concept in its own right, and talking about its constituent parts using industry language. Hence, the use of the simpler term “responsible innovation”, acknowledging the overlap with the more familiar concept of corporate social responsibility.
- Being clear about the benefits of ethical approaches in commerce.
- Making a positive effort to understand the commercial context within which SMEs operate (i.e. through engaging in or speaking at their events), rather than expecting them to come into the academic world.
- Engaging with external advisory organisations to boost credentials and trustworthiness.
- Extending academic knowledge around responsible innovation and ethics in order to understand the key technical and commercial dilemmas, challenges and opportunities that confront companies in the sector in question.
- Minimising the requirements for companies to participate (e.g. time, travel, etc.).
- Being positioned to assist with any particular ethical dilemmas or issues faced by the companies.
- Engaging in personalised and often face-to-face discussions with key members of the companies in order to demonstrate understanding, and to establish a rapport conducive to outcomes within workshops.

Some of these approaches may be more specific to cyber security companies, but there are wider lessons for other sectors. Perhaps most notable (and generalisable) is the importance of understanding the sector in question and its commercial context in order to engage with the staff, often at a senior level, of SMEs. This positions the researcher more clearly as an equal in the search for insights and truths that the workshops can reveal. Linked with this is the need not to offer RI as a model or blueprint, but rather to demonstrate knowledge of the sector; personalise and tailor information to the specific company; and to focus on those components of RI which are already recognised by the company.

Image Credits Tower by iconcheese from the Noun Project
contract by Templet from the Noun Project
consulting by Vectors Market from the Noun Project
Tailor by Pham Duy Phuong Hung from the Noun Project
Recruitment by Massupa Kaewgahya from the Noun Project
Conversation by Olivia from the Noun Project

Appendix

Dear _____,

As a security company, you're probably very concerned about ethics, and ensuring your business acts as responsibly as possible. What we want to do is to help your company be even more ethical in your business practices.

We want to be pragmatic, useful, and responsive to your company's needs and goals.

Much like the security sector sells an idea – that security needs to be built in from the beginning – we will convince you that if you build in responsible and ethical practice from the beginning, you'll benefit from it in the medium-long term through:

- better relationships with clients;
- broader and more sensitive outreach and sales approaches;
- higher levels of client trust in your company;
- a more embedded community presence;
- and an agility for future challenges and opportunities.

We will work directly and confidentially with you and your company, identifying your areas of good practice and injecting good practice identified by interviews with practitioners, CEOs, and developers of other tech companies. We have successfully done this with the health technology sector in the past, and now we want to open up our methods to the security sector.

We want your company to be prepared for what the future might bring – 2, 5, even 10 years down the line, and help you to put good practice in place to be able to deal with these challenges and opportunities. You'll also learn how to use our techniques to help potential clients think about their own futures – and how security can benefit them.

We'll need around 5 h of your time total, spread over 2 face-to-face meetings where we come to you, and a couple of short follow-up phone calls/emails after each meeting. In between, we will integrate expert opinion from our research for the COMPASS project, the East Midlands Police, academic security researchers, business support organisations such as B Labs and EBN Innovation Network, and professional organisations to help you look above and beyond your everyday practice.

You'll get a tailored, future-looking roadmap to practically implement responsible and ethical practice in your company, so you can benefit from being more trustworthy, learn from our methods, and end up with a more agile, future-looking company that can be relied on by customers and the public to behave ethically and responsibly.

For more information please contact ...

Sincerely,

References

- Department for Business, Energy & Industrial Strategy. (2017). UK innovation survey 2017: headline findings [WWW Document]. GOV.UK. <https://www.gov.uk/government/statistics/uk-innovation-survey-2017-headline-findings>. Accessed 11.8.18.
- European Commission. (2011). A renewed EU strategy 2011–14 for corporate social responsibility', Communication from the commission to the European Parliament, the council, the European economic and social committee and the Committee of the Regions COM/2011/0681 final.
- European Commission, Directorate-General for Research and Innovation. (2013). *Options for strengthening responsible research and innovation*. Luxembourg: EUR-OP.
- Hughes, M. (2015). *Full or responsible disclosure: How security vulnerabilities are disclosed* [WWW document]. MakeUseOf. <http://www.makeuseof.com/tag/responsible-disclosure-security-vulnerabilities/>. Accessed 13.12.17.
- Lefkowitz, J. (2017). *Responsible disclosure – Critical for security*. Critical for Intelligence | SecurityWeek.Com [WWW Document]. URL <http://www.securityweek.com/responsible-disclosure-critical-security-critical-intelligence>. Accessed 13.12.17.
- Owen, R., Stilgoe, J., Macnaghten, P., Gorman, M., Fisher, E., & Guston, D. (2013). A framework for responsible innovation. In R. Owen, J. Bessant, & M. Heintz (Eds.), *Responsible innovation* (pp. 27–50). Chichester: Wiley. <https://doi.org/10.1002/9781118551424.ch2>.
- Stahl, B., Flick, C., Mantovani, E., Borsella, E., Porcari, A., Barnett, S. J., Yaghil, A., Ladikas, M., Hahn, J., Obach, M., Garzo, A., Schroeder, D., Chatfield, K., Antoniou, J., Paspallis, N., Brem, A., Yaghmaei, E., Brey, P., Søraker, J. H., Gauttier, S., Gurzawska, A., Ikonen, V., Leikas, J., & Mäkinen, M. (2017). Benefits of responsible research and innovation in ICT for an ageing society. *Responsible-Industry Project*. <https://doi.org/10.5281/zenodo.1050357>.
- Von Schomberg, R. (2013). A vision of responsible research and innovation. In R. Owen, M. Heintz, & J. Bessant (Eds.), *Responsible innovation. Managing the responsible emergence of science and innovation in society* (pp. 51–74). Wiley.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

