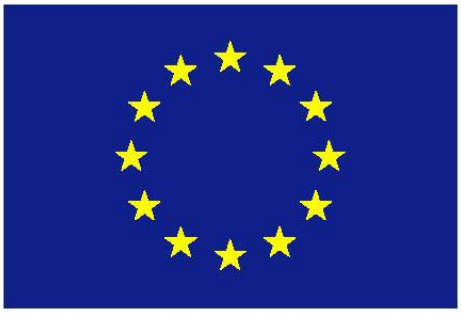
Global Model and Observatory for International Responsible Research and Innovation Coordination

D 3.3 Briefings Report



"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 321489"

D 3.3 Briefings Report			
Document No.		3.3	
Workpackage No.	WP3	Workpackage Title	Forum
Start Date:	20	Revision Date:	2.0
Author(s)		Menisha Patel, Marina Jirotka (Oxford)	
Editor		Mohamad Ajami (Fraunhofer)	
Contributors			
Status		R, PU	
Date		22 March 2016	

* R = Report, P = Prototype, D = Demonstrator, O = Other PU = Public, PP = Restricted to other programme participants (including the Commission Services), RE = Restricted to a group specified by the consortium (including the Commission Services), CO = Confidential, only for members of the consortium (including the Commission Services).

No.	Partner Name	Logo
1	Fraunhofer IPK	
2	Signosis Sprl	
3	De Montfort University	
4	University of Namur	
5	Technical University of Berlin	
6	University of Oxford	
7	GeoImaging Ltd	
8	University Sienna	
9	University of the Aegean	
10	University Malaysia Sarawak	
11	Universidad de Chile	
12	Kyushu Institute of Technology	
13	Arbeiter Samariter Bund Wien Gesundheit und Soziale Dienste Gemeinnützige GmbH	

Table of Contents

List of Tables

Executive Summary

An important aspect of the RESPONSIBILITY project in being a coordination and support action is to engage with wider stakeholder communities. This is in particular relation to raising awareness of and providing recommendations regarding how RRI can be embedded into the practices, procedures and products in relation to research and innovation.

Through this deliverable, we detail the development of a tool that we see as important for bridging the gap between research evidence, and policy makers and industry. More specifically, we outline the development of reflection papers geared towards providing RRI-oriented recommendations to these stakeholder communities. We discuss how three policy reflection papers and one industry reflection paper were created. We then go on to present the papers themselves. Finally, we briefly outline how such papers can be embedded into the Observatory (developed through WP4), or even developed further to constitute policy or Industrial reflexion documents for formal release.

1 Introduction

Since the RESPONSIBILITY project is a coordination and support action, then ensuring practical relevance of the project is an important feature of our work.

Broadly speaking the development of the online prototype platforms the Forum (primarily through WP3) and Observatory (primarily through WP4) have been important elements in providing a crucial infrastructure to support the creation and maintenance of a network of stakeholders for the consideration of, and diffusion of RRI. What is also an important aspect of engaging with the broader community of stakeholders (including stakeholders and industry) has been the creation and collection of materials such as case studies (D2.3) that have been used to begin to populate the Observatory (and are linked to the Forum through a related content function).

Through this deliverable the production of another genre of materials to engage with the wider community of stakeholders is discussed. More specifically, the production of three policy reflection papers and an industrial reflection paper that recommend (in various ways) the need to integrate the principles of RRI into particular policy/industry actions is detailed.

Akin to more lightweight versions of formal policy brief documents: such reflection papers may serve as important tools for informing wider stakeholders (including primarily policy makers and also members of industry) of how RRI can provide a response and possible solution to dealing with various problematic issues in particular domains of concern. Aside from an RRI-oriented shaping of recommendations, the recommendation papers also serve as tools to disseminate awareness regarding the importance of RRI as an integral and necessary consideration for practices, procedures and tools in relation to research, innovation and industrial products and processes (depending on the nature of the subject area).

The RESPONSIBILITY reflection papers have been developed iteratively through the expertise of selected members of the consortium. The particular subject areas of focus for each of the papers were informed by in-depth deliberation within the project consortium, in order to determine what were considered key areas of topical and current relevance to RRI. Importantly considerations were also shaped by what was seen to be expert knowledge areas of partners involved in the task- that would play a significant role in ensuring the quality of the final papers produced.

The policy reflection papers concern the following areas:

Cloud Computing and Privacy
Civil Drones and Regulations in the EU: Current use, regulations and potential concerns
RRI for Security

There has also been an industry reflection paper produced:

RRI Approach in Engaging Stakeholders for Sustainable Palm Oil in Malaysia

We briefly outline the importance of these papers as tools for communication with wider stakeholders and informing the decisions of policy makers in relation to suggesting the integration of RRI and its related principles into their considerations, and then go on to

detail the manner in which they were produced. The reflection papers themselves are then embedded into the report, and finally we outline what future plans could involve in relation to the dissemination of these papers. It also vital to mention, that given the nature of the comments by the reviewers in the mid-term review, and the comments regarding the categorisation of the document, the term briefs was replaced by reflexion in order to insure a smooth released of this document, which is due to be included in a post project dissemination phase

It is envisaged that *at the very least* the reflection papers will be embedded within the RESPONSIBILITY Observatory to form part of the growing corpus of materials (including, for example: case studies) that have already been placed on the platform.

2 An introduction to the Policy and Industry Reflection Papers

The reflection papers produced through this project are short documents that present findings and recommendations to particular stakeholders in relation to providing information, evidence and recommendations for dealing with issues seen to be of importance. The policy reflection papers are aimed at government policymakers and others who are interested in formulating or influencing the policy issue(s). It is foreseen that they may provide a key communication tool that links researchers' findings to policy actors. Thus through RESPONSIBILITY they are considered to be an important dissemination tool for stakeholders. Importantly through this project we have also produced an industry reflection paper geared towards industrial stakeholders. The purpose of this industrial reflection paper is to outline key concerns regarding the production of palm oil and the recommendation that RRI is embedded into organisational practices and procedures in order to mitigate this detrimental impact.

Better use of research based evidences of the scientific expertise to policy makers and industrial stakeholders could significantly help to tackle societal challenges and effectively address or anticipate the demands of the population in need. Given this important bridging role they can play, in making research evidence and outcomes more accessible to other stakeholders, then the reflection papers provide an important tool for the recommendation that RRI be embedded into the consideration and development of various issues.

As mentioned, there have been four reflection papers produced as part of RESPONSIBILITY. Through this section we reveal how they were produced.

2.1 The Production of the Reflection Papers

The three policy reflection papers and an industry reflection paper were produced according within three broad iterations. An iterative approach was seen as important for a considered and deliberative process of production: through which drafts of the briefs could be scrutinised and evaluated to facilitate the development of good quality materials.

Before the three iterative stages of development were undertaken, there was a period of consideration by the consortium as a whole; in relation to which particular subject areas would be most appropriate for the papers to provide information and recommendations upon. Discussion and decision-making was informed by what were seen to be particularly topical issues at the time of consideration, and the expertise of the consortium. For example, in relation to the industry reflection paper: given the involvement in the consortium of a Malaysian partner which expertise and understanding, and the widely publicised controversies regarding palm oil, then it was seen that this was an important contribution that RESPONSIBILITY could make in providing information to relevant industrial partners.

Following this decision making process, partners with appropriate and complementary expertise who were designated to the task (T3.3), were separated into three sub-groups, each asked to lead the development of specific papers. These groupings were as follows:

Table 2.1: An outline of responsible partners

Brief	Responsible Partners
Cloud Computing and Privacy	Aegean
Civil Drones and Regulations in the EU: Current use, regulations and potential concerns	Fraunhofer, Aegean
RRI for Security	Fraunhofer
RRI Approach in Engaging Stakeholders for Sustainable Palm Oil in Malaysia	UNIMAS, Fraunhofer

The groups were firstly asked to outline in a long and discursive document, what the particular concerns and issues were in relation to their topic area. These were then considered by the wider consortium in order to provide feedback regarding what the broad shape and core argument that the reflection papers may take.

Following this first iteration, the groups were provided with a policy template (see Figure 1, below), which had been created through WP6, for use in T6. Xx. This provided them with the structure that their brief should follow, and the points that each aspect of their paper should consider.

Table 2.2: The policy reflection paper template

Title of the policy reflection paper	
Executive Summary	• Description of the problem • Why current policy needs to be changed? • Recommendations for action • What the outcome might be? (If recommendations are followed)
Problem Description	• Statement of the problem • Short overview of root causes of the problem • Policy implications of the problem to highlight current importance and policy relevance • What is at stake? (Competition, situation, benchmark, examples, resources needed, trade-offs)
Policy Options	• Short overview of policy actions in focus • Argument for why and how current action is failing (examples) • Where are the linkages?
Policy Recommendations and Conclusions	• Specific practical steps to be implemented (the most critical part of the policy reflection) • Based on an example of a failure and a success • Closing paragraph emphasising action's importance
Appendices	• Only to be included when absolutely necessary

Bibliography	• A short bibliography would be included if necessary
Key Points • The paper should be kept short and concise- an overly complex policy reflexion will not be desired by EU policy makers- maximum ten pages (policy paper guide- attached) • The policy paper will use different language, and be geared towards a different 'audience' to the industry brief- it is worth beginning to consider where we can find sources of industry briefs- and how these are constructed semantically.	

The industry reflection paper template was informed by the policy paper template. This is as the core components of the template were seen as important in constituting what an industrial paper (oriented towards relevant industrial stakeholders) should incorporate.

Table 2.3: The Industrial reflection paper template

Title of the Industrial paper	
Executive Summary	• Description of the problem • Why current Industrial measures need to be changed? • Recommendations for action • What the outcome might be? (If recommendations are followed)
Problem Description	• Statement of the problem • Short overview of root causes of the problem • The influence of this industry on the problem indoor to highlight current relevance • What is at stake? (Competition, situation, benchmark, examples, resources needed, trade-offs)
Industrial measures	• Short overview of measures and actions in focus • Argument for why and how current action is failing (examples) • Where are the linkages?
Industrial Recommendations and Conclusions	• Specific practical steps to be implemented *(the most critical part of the paper)* • Based on an example of a failure and a success • Closing paragraph emphasising action's importance
Appendices	• Only to be included when absolutely necessary
Bibliography	• A short bibliography would be included if necessary
Key Points • The Industrial paper should be kept short and concise- an overly complex policy reflexion	

will not be desired by EU policy makers- maximum ten pages (policy paper guide- attached)

- The policy reflexion will use different language, and be geared towards a different 'audience' to the industry brief- it is worth beginning to consider where we can find sources of industry briefs- and how these are constructed semantically.

Following the second and third iteration of the development of the papers, they were evaluated according to an evaluation template. This template was developed according to the recommendations of the EU DESIRE Project (http://www.desire-his.eu/es/descargas/doc_view/193-guidelines-to-writing-a-policy-brief), and well as the original production templates provided to the sub-groups for the development of each paper. The evaluation template appeared as follows:

Table 2.4: Policy/Industry Reflection Paper Evaluation Template

Section Name	Evaluation Points	Yes (Tick if you agree that point has been addressed)	Comments
1. Title The title is the reference point of the entire paper, so should clearly reflect the content.	Is the title of the paper relevant to its content?		
	Does the title clearly demarcate the central issue?		
	Does the title entice policy makers/members of industry to read on?		
2. Executive Summary The executive summary should convince the reader that the brief is worth reading.	Is it of adequate length? (1-2 paragraphs)		
	Is there a clear description of the issue and why there is a need for action now?		
	Is there a clear recommendation of what action should be taken?		
	Is there a clear indicator of what the outcomes may be if the recommendations are followed?		
3. Problem Description The purpose is to convince the target audient that a current and urgent problem exists and requires action.	Is there a clear indication of what the problem is?		
	Is there a clear indication of what the root causes of the problem are? (if necessary what has been done to address them so far)		
	Is there a clear the current importance, urgency and policy/industrial relevance of the issue?		
	Is there a clear description of what is at stake if the issue is not dealt with?		

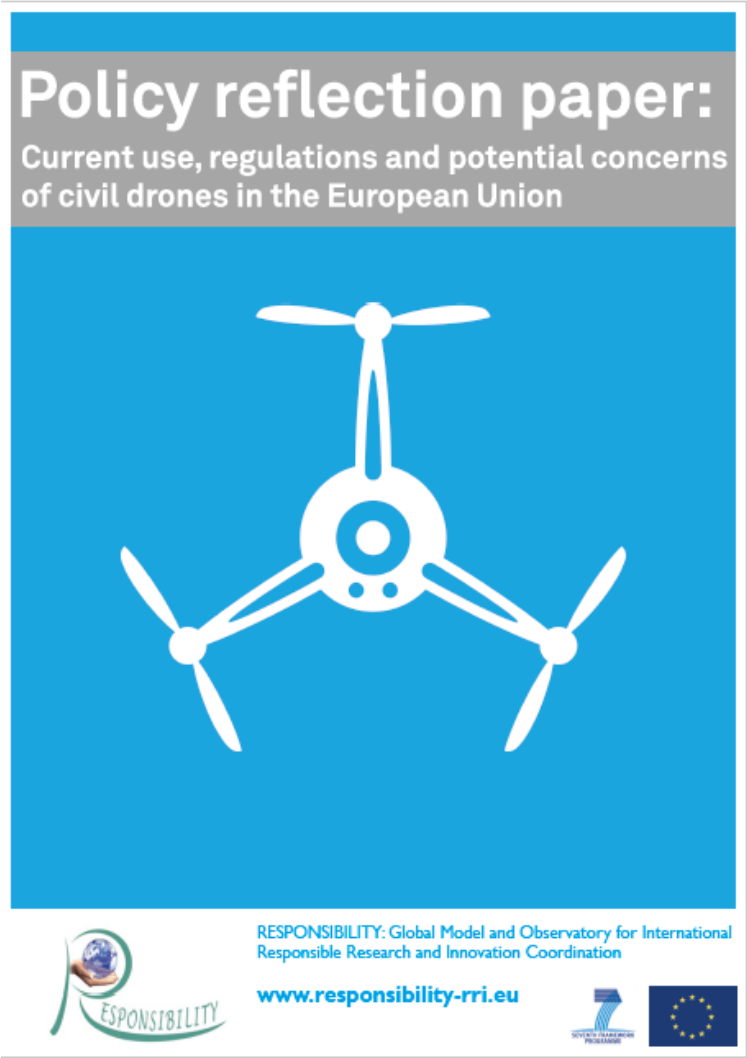
Section Name	Evaluation Points	Yes (Tick if you agree that point has been addressed)	Comments
4. Policy/Industrial Options This section should detail shortcomings of the current approach, and illustrate both on the need for change and the focus of where change should occur- critiquing current policy/industry options in doing this.	Is there a short overview of policy/industry options that could be used to deal with this?		
	Is there an argument for why and how the current or currently proposed approaches are failing- and details of advantages and disadvantages of each of these options?		
5. Policy Recommendations and Conclusions Should be a detailed and convincing proposal of how the failings of the current policy/industry approach need to be changed- and importantly what these changes are.	Is there a detailed and convincing proposal of how the failings of the current policy/industry approach need to be changed?		
	Is there a clear repetition of the key message, and an outline of what actions need to be taken and why? (Importantly this should be related back to previous sections; could include timescales of action).		
	Is there a closing paragraph emphasising the importance of action?		
6. Appendices Should only be included when absolutely necessary	Is it essential to include these appendices?		
	Is this section clearly labelled and organized?		
7. Bibliography	Is this section necessary and neatly organized?		

Section Name	Evaluation Points	Yes (Tick if you agree that point has been addressed)	Comments
8. General Issues	1. Is the paper written in accessible language (as policy/industry makes will not necessary be expert in this particular area)?		
	2. Does the content link to actual policy/industry debates?		
	3. Does the brief summarise the current debate well, does it give a brief but complete overview?		
	4. Are any normative (one-sided, unbalanced) words used like “have to”, “unacceptable”, and “deplorable”? Try to replace them with the underlying argument instead (why it has to be done, what makes something unacceptable or deplorable). It is necessary to present arguments that convince others who might not necessarily have the same norms and values. Also, superlatives and emotive language can be quoted out of context.		
	5. Does the paper contain concrete policy/industry recommendations that are derived logically from the arguments?		
	6. Is the composition of the paper logical? Are all parts needed for the story and do they logically follow one another?		
	7. Is the content of the paper less than eight pages? (this should be a maximum- excludes appendices and references)		

3 The Policy and Industrial Reflection Papers

In this section we now go on to present each of the reflection papers that was produced: more specifically, the three policy reflection papers followed by the industry reflection paper on palm oil.

The first paper to be presented entitled *Civil Drones and Regulations in the EU: Current use, regulations and potential concerns,* has been aesthetically shaped beyond MS word format, by the consortium partner GeoImaging Ltd. This is to give a further indication of the aesthetic standard of a paper for formal dissemination to relevant stakeholders. It is recognised that the content as well as the aesthetic presentation of the paper will play an important role in the appeal of the target stakeholder community to read and consider the materials and ideas presented.



The other papers are presented in MS word format, and it is envisaged that upon formal release they too will be developed aesthetically.

3.1 Policy Reflection Paper 1: Civil Drones and Regulations in the EU: Current use, regulations and potential concerns

1. Executive Summary

Remotely Piloted Aircraft Systems (RPAS) for civil applications, which are also known as Civil Drones, are becoming increasingly popular and a controversial discussion is arousing relatively to their use. They are progressively integrated into the European civil airspace to perform numerous applications ranging from leisure, services, photography, logistics and surveillance. Especially, since the RPAS technology has matured rapidly in past years, and as like many other aircraft technologies before it is ready to make the shift from being purely military equipment to becoming a reliable new technology for civil use.

RPASs have an undeniable and substantial value for a wide range of purposes such as for search and rescue or the so called "eco drones" that are used to monitor deforestation and poaching and can also assist in precision agriculture to map coastline erosion to species and habitat monitoring. Despite this value, their use poses new challenges related to safety, security and respect of citizens' rights with focus on their privacy. The lack of harmonized regulations across Europe and the inefficiencies of current policies impose actions to ensure the integration of RPAS for public use. Extensive research of lessons-learned, legislative proposals to remove uncertainties and modifications in current policy regulations are required. Directives are also needed on a European level to follow and support future development and usage of RPAS geared to the common good.

3.2 Policy Reflection Paper 2: Cloud Computing and Privacy

1. Executive summary

Cloud Computing is one of the major developments of Information and Communication Technologies (ICTs) in 21st century. Despite the various efficiency benefits and resource savings that enables the migration of business and governmental organisations towards cloud computing, yet a major concern is still about the implications on privacy and data protection rights. The European legal framework, mainly the General Data Protection Legislation, and the cloud specific key actions of the European Union are useful but not sufficient tools to deal with privacy issues in cc. Common understanding and deliberation on issues such as security requirements and privacy needs will enable to assess impacts and to mitigate risks through identifying, balancing and/or harmonising competitive rights and interests. In this context it is a prerequisite to build consensus among all stakeholders, including citizens, public administrations, and the cloud industry and users. Respective recommendations are addressed to all stakeholders, namely governments in their capacities both as regulators and users of cc services, industry, research communities/ organisations and individual users. Emphasized is the need for adopting clear and cloud adequate rules, complemented and supported by self-regulatory framework and codes of conduct. Moreover discussion and guidance on particular issues will allow stakeholders to develop and adopt principles, standards and good practices and integrate these into research and innovation processes with regard to cloud computing.

2. Problem Description

2.1 Cloud computing: a major game-changing technology

Cloud computing (CC) has reached unexpected heights in the last years and is recognized by governments and private-sector organizations as a major game-changing technology. CC is *"a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* (US National Institute for Standards and Technology (NIST) [1].

Cloud computing is characterized by flexibility enabling the identification of cloud models and solutions that are appropriate depending on customer needs, the type of processing and their compliance requirements. By transforming the way technology is delivered, cloud computing is promising remote, rapid, efficient and cost-effective deployment of computational resources (hardware/software) across different (economic) domains and geographic areas, enabling market entrance with global reach [2]. By making computing power available everywhere and to anyone [3], *CC is expected to contribute to* remarkable cost and efficiency savings, up and down scalability, flexible capacity, reallocation of staff and resources and to reshape the Information Technology marketplace.

Cloud computing enables a new platform and location-independent perspective on how we work collaborate and communicate: Users actually use on a daily basis cloud services to store information (e.g. pictures or e-mail) and/or to interact in social networks or access streamed video and music or games). As in the case of GRID technologies, cloud computing can provide high capacity and dependable infrastructure that can be used to scientific research. Cloud computing services enable coordinating and sharing of resources under standard, open, general purpose protocols and interfaces [4].

Taking into account both the increasing demands for IT solutions and the challenging economic conditions, the value proposition of the cloud seems to be especially appealing for governments, which may become the leading sector in the development of cloud computing. Public administrations can obtain significant efficiency gains from wide-scale adoption of cloud computing, as it allows offering e-government solutions, independently of divergence of local administrative units that may be better or worse prepared to provide e-government services [5].

2.2 Controversial dimensions - Cloud computing and privacy/ Privacy in cloud: cloudy privacy?

Cloud computing offers an impressive range of possibilities but it also raises challenges for both individuals and organisations in private and public sector. Despite providing substantial benefits, this "backbone technology of the Future Internet" [6] triggers privacy and security concerns at all levels. Security risks and breaches, unauthorized access to legally protected information with focus on personal data, compliance with legal requirements, accountability and liability of cloud customers and providers are the issues raised by businesses, Data Protection Authorities and individuals [7]

Cloud computing services, both in form of storage facilities and processing requests, lead – almost by definition - to the aggregation of large amounts of (personal) data especially in the hands (data centres) of big cloud computing providers risking to interfere with the rights and interests of individuals]. This aggregation is more likely to harm individuals when the cloud providers' business model is based on commodifying personal information. In cloud computing environments personal data may be deployed, disassembled and/or reassembled on a wide scale across a highly distributed infrastructure, which may propagate the risk of a lack of control over personal data as access, editing or retrieval thereof requires the participation of the cloud provider. This "loss of control" (or perhaps the feeling thereof) relates also to the difficulty for the cloud customer to know and effectively check the data handling practices and data processing carried out by the cloud provider [8]. This feeling is especially the case regarding individuals who often store and process sensitive data when using cloud computing services in the context of social media applications as many Cloud Computing providers are technically able to perform data mining techniques to analyse users' data.

Another concern of (potential) cloud customers and users is often related to an (inherent) characteristic of cloud computing : the multiple locations of data (centres) and data transfers associated with cloud computing raise questions of (lawful) trans-border data flows, oversight and the applicable law. Difficulties to define applicable law are also related to uncertainties concerning the multiple and different roles of actors involved (cloud providers, cloud sub-providers, cloud customers/users, intermediaries) and their respective rights and interests, responsibilities and liabilities. This cloud value chain is both complex and dynamic and the involvement of sub-processors in the cloud processing chain may infringe the rights of the cloud computing customers especially if they have not consented to or even they are not aware of (it).

Furthermore users' concerns relate to information systems as well as network security of cloud computing services and especially confidentiality of data communicated between cloud provider and client as well as between data centres. Users may also be concerned about the handling of their personal data by the cloud provider: the fear that cloud

providers may mismanage their data or (miss)use them for purposes not authorized by the user profiting from its privileged access rights to link personal data from different customer/clients and sources [8]

2.3 Mistrust and Uncertainties

The multiplicity of locations results to further uncertainties concerning the applicable law and jurisdiction which on their turn result to difficulties pertaining to compliance checks and law enforcement. Legal uncertainty undermines not only the use of cc services. Privacy concerns und uncertainties about…location of data, the allocation of roles…and the applicable undermine the trust to cloud computing and cc providers and constitute "one of the most serious barriers for cloud computing take up" [3]

Governmental agencies are, however, often very hesitant to adopt cloud solutions, because of information security and privacy concerns, since lack of trust has indeed proven to be one of the significant barriers limiting the wide adoption of cloud computing. It is Important to deal with these issues and concerns is critical, as they may refrain business, public sector as well as individuals from migrating to the cloud. With further impacts on growth of digital economy, the tension between benefits of CC and security/ informational privacy considerations and respective requirements has to be balanced, if not resolved, also through coupling of integrated processes of anticipation, reflection and deliberation to policy and decision making processes.[9]. Achieving a balance of innovation and growth with the need of guaranteeing fundamental rights is one of the challenges RRI has to face.

3. Policy Options

3.1 Cloud Computing Strategy and the General Data Protection Regulation

The European Cloud Computing Strategy as expressed in 2012 by the European Commission's Communication "Unleashing the Potential of Cloud Computing in Europe", aims not only to ensure that Europe can profit from the shift to cc but also to improve the clarity and increase the understanding of SLAs for cloud services in the market as well as of critical areas of cloud computing in connection with security or personal data protection.

In this context the European Commission has launched initiatives such as the creation of a high level Steering Board and the elaboration of Cloud Service Level Agreement Standardisation Guidelines [10] The European Union has identified cloud-specific Key Actions in the Europe 2020 plan that include the standardization of SLAs, the Safe and Fair Cloud Contract initiative and the drafting of a data protection Code of Conduct. Another aspect of the European cloud policy refer to the developing of standards and certification schemes in collaboration with European Union Agency for Network and Information Security (ENISA), industry and other relevant bodies to implement actions on standards, certification, contract terms and conditions and a European Cloud Partnership. The efficiency of these key actions is dependent on identifying and counteracting typical risks and challenges like the availability of services and data, the current lack of data classification mechanism, integrity issues, confidentiality concerns, regulatory compliance, reputability, loss of control, responsibility ambiguity, lack of liability [11]

The General Data Protection Regulation as adopted in December 2015 does not contain any cloud specific provisions, which is to attribute to the choice of the so called "technological

neutrality" of the proposed provisions. However, some of the draft provisions/set of provisions such as these concerning the allocation of responsibilities between data controllers and data processors and the territorial scope or the new European Data Protection Law may have impact on the regulation of cloud computing (services): However, the Regulation must be capable of internalising pending technological paradigm shifts, such as cloud computing, and be sufficiently flexible to apply to new data-driven business models [12].

3.2 Failure of current action

The current policies and actions are a necessary but not sufficient condition for aligning their outcomes to stakeholders concerns. As Cloud computing has reached a wide range of users (including public sector, SMEs and individual users) that due to characteristics / features of cc (imbalance of powers, multiple locations/jurisdiction, lack of transparency) are - normally - hardly in a position to articulate their concerns and needs. Identifying stakeholders/ societal actors that should be targeted in cloud computing environment is a first crucial step. As cloud computing is a multidimensional horizontal technology the scope of involved actors and stakeholders can be very wide, a first major distinction being this of cloud providers and cloud customers.

The most ubiquitous requirements for trust building are information security and compliance with privacy and data protection rules and principles that have to be guaranteed and steadily reassured by a multiplicity of stakeholders: the cloud providers, the cloud customers, legislators and oversight bodies. More than elaborating standards, certification schemes , contract terms and conditions and data protection provisions what is needed is a comprehensive/holistic and multidisciplinary approach that with the involvement of stakeholders and other interested parties should lead to an inclusive research and innovation process. Such a process would contribute to cloud computing services providers and researchers becoming responsive to societal needs, compliance requirements and privacy concerns and expectations and stakeholders becoming aware and responsible for input in terms of defining desirable ways of providing and receiving/ enjoying cloud computing services, while preserving their fundamental rights and interests.

4. Specific practical steps to be implemented – Recommendations

4.1 Deliberation

Reflecting on the importance of these issues, it is imperative for the relevant stakeholders (businesses, public organisations but also individual users) to be well-informed about the issues raised concerning privacy and data protection issues related to cloud computing applications and services and they possible ways/ approaches to deal with. In-depth deliberation related to the impacts of cloud computing on privacy is vital to ensure holistic understanding can be attained for the purpose of re-examining the existing policies and practices of organizations (both private and public sectors) in subscribing and using cloud application and services. Discussion and guidance on particular issues will allow stakeholders to develop principles and standards of good practice and integrate these into research and innovation processes with regard to cloud computing. [13]

4.2 Innovation and protection through clarity and legal certainty - Privacy Protection and Trust by regulatory intervention

the active role of the regulators remains central to establish legal certainty as clarifying and making the regulatory framework of data protection more effective and appropriate for cloud computing environments lie out of the range of the other actors involved, i.e. cloud users/customers and cloud providers. Governments have to get actively involved in the discussion about balancing benefits of cc and assuring fundamental rights assume their regulatory role more actively. [14]. Accessible, clear, unambiguous and at the same time flexible and enforceable regulatory framework and contractual clauses are significant conditions for the social acceptability and the adoption of cloud computing services. Legislators have to foster the position of individuals by introducing clear and consistent rules and Data protection authorities have to enforce compliance with data protection and security requirements Technology neutrality should be a guiding principle both for regulating and interpreting the law.

4.3 Involvement of non–legislative bodies to promote impact assessment and accountability measures.

Any regulatory attempt and intervention should be complemented by a policy, which includes and engages in consultation non-legislative regulators, supervisory bodies, professional bodies and industry associations**.** These bodies should be encouraged to ensure that their guidelines and policies are at least cloud neutral (i.e. enable cloud services) wherever this is compatible with their goals.

Taking into consideration the difficulties by identifying and applying the law, self-regulation could increase professional reputation, while preserving ethical standards and restoring trust. This can be achieved, for instance, by promoting certain good practices (interoperability, privacy-compliant applications and services, etc.) and banning others types of activities that may interfere with the users' rights (user-profiling, targeted advertising, lack of transparency concerning sub-contractors etc.).

Concerns have been expressed with regard to the outcome and efficiency of self-regulatory efforts given the characteristics and the structure of the market of cloud services, that is dominated by few and large corporations. Therefore a kind of co-regulation or regulated self-regulation has to be recommended: The State can provide the necessary incentives for Cloud providers to regulate themselves in a way that properly takes into account users' demands and expectations [15] and adopt the measures the promote accountability [2]. In this perspective it is important to support also the user's position and offer the tools for articulating their expectations in the process of achieving a common understanding.

4.4 Privacy Impact Assessment, privacy by design and standards

Guidelines and policies have to be grounded on assessment of risks and benefits, of impacts and effects on privacy. The identification of the risks related to the personal data processing in cloud environments, their assessment in terms of their origin, nature, likelihood and severity is necessitated for identification of measures and best practices to mitigate these risks. Industry, in collaboration with relevant civil society stakeholders may develop a framework for privacy and data protection impact assessments [16]. The European Commission could develop templates that could be used to evaluate and manage risks in

cloud computing to provide incentives to engage with relevant issues and encourage discourses that may lead to the development of specific policies and responsibilities [17].

With regard to the protection of individuals' rights and freedoms and especially privacy, methodologies have been developed that aim at integrating regulatory requirements into research and innovation, with the most relevant example being the idea of "privacy by design" [18] that aims at embedding privacy and data protection into the design of this technology or system.

In this context operational guidelines and technical standards are recommended to enable compliance with security and privacy issues. Embodying a consensus about how to do something based on accumulated experience, cloud standards may ensure both a competitive and open market between cloud suppliers and protection of security and privacy. To highlight is the adoption (2014) of ISO/IEC 27018, an International Standard which establishes commonly accepted control objectives, controls and guidelines for identifying security risks and implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. Standards may be adopted voluntarily, negotiated or mandated on a cloud provider, or the sector as a whole, through both public and private law mechanisms. In this context, a necessary component of this strategic choice that could be supported by RRI tools is raising awareness about the processes through which values and norms become embedded in the technological architecture.

4.5 Consensus and best practices

A framework for effective data protection in the cloud consists not only of legal measures and guidelines but also of consensus building among all stakeholders, including cloud providers and cloud users, citizens and public administrations (especially data protection authorities) [19].]A very crucial tool/element for consensus and trust building is the identification and promotion of best practices by the cloud industry in respect of compliance with the law, security, technical standardization and operational assurances. The flexible common framework of best practices that is suggested should consist of both legal and operational guidelines as well as technical standards and could voluntarily adopted by cloud providers to show that their services comply with the common framework and to help cloud customers and users to choice a privacy responsible cloud supplier.

5. Conclusion

Cloud computing is a key enabler for growth and has the potential to bring significant services and advantages to citizens, businesses and public administrations. This policy reflexion, aims to respond to the need to provide a balanced view where relevant stakeholders of cloud computing applications and services can benefit from cloud computing opportunities and at the same time be well-informed with regard to the impact of the technology on informational privacy rights in order to appropriately face these challenges and mitigate the privacy risks. Policy makers and innovators should consider how to institutionalize important discourses that allow stakeholders to engage on a content level with the policy – as well as technical – community through establishing a forum for stakeholders' involvement (and especially the powerless individual users) that should ensure that innovation and service offering in cloud ecosystem reflect also societal concerns and balance competing rights and interests. RRI could be used as an instrument to assess

impacts and to mitigate risks through identifying, balancing and/or harmonising competitive rights and interests and as a sensitizing tool to re-examine the existing policies and practices in reflection to what are being highlighted, discussed and recommended in this policy reflexion to strengthen privacy protection in cloud computing environment.

Bibliography

[1] P. Mell and T. Grance, 'The NIST Definition of Cloud Computing', National Institute of Standards and Technology, 2009. Accessible at http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[2] Felici, M., Jaatun, M. G., Kosta, E., & Wainwright, N. Bringing Accountability to the Cloud: Addressing Emerging Threats and Legal Perspectives. In Cyber Security and Privacy, (2013). Springer Berlin Heidelberg, pp. 28-40

[3] European Commission, Communication Unleashing the Potential of Cloud Computing in Europe, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Brussels, 27.9.2012 COM(2012) 529 final (2012)

[4] BRIE Working Paper

[5] Glott, R., Husmann, E., Sadeghi, A. R., & Schunter, M. Trustworthy clouds underpinning the future internet. Springer Berlin Heidelberg. (2011), p. 209)

[6] D. C. Wyld, The Cloudy future of government IT: Cloud computing and the public sector around the world. International Journal of Web & Semantic Technology, 1(1) 2010, pp. 1 ff

[7] Art 29 Data Protection Working Party, Opinion 5/2012 on Cloud Computing

[8] ENISA, Cloud Computing- Benefits, Risks and Recommendations for Information security, 2009,

[9] Richard Owen1, Phil Macnaghten2 and Jack Stilgoe1 – Responsible Research and Innovation: from Science in Society to Science for Society, with Society

[10] The Cloud Select Industry Group – Subgroup on Service Level Agreements (C-SIG-SLA). Letter to European Commission, June 25 2014]

[11] Manfred Halper/Stefan Fenz/Johannes Göllner/Gerald Quirchmayr Evaluation criteria for cloud computing based on the upcoming European data protection regulation]

[12] Irion K. and Luchetta G.,(2013) Online personal data processing and EU data protection reform online at http://www.ceps.eu/book/online-personal-data-processing-and-eu-data-protection-reform]

[13] Bernd Carsten Stahl Responsible research and innovation: The role of privacy in an emerging framework Science and Public Policy (2013) pp. 1–9

[14] Urs Gasser and David R. O'Brien Governments and Cloud Computing: Roles, Approaches, and Policy Considerations

[15] De Filippi, P, Belli, L, 'Law of the Cloud v Law of the Land: Challenges and Opportunities for Innovation', European Journal for Law and Technology, Vol. 3, No. 2, 2012]

[16] Wright D.-De Hert P., Introduction to Privacy Impact Assessment, . Wright D.-De Hert P, Privacy Impact Assessment…p. 6

[17] Bernd Stahl, Marina Jirotka, and Grace Eden Responsible Research and Innovation in Information and Communication Technology: Identifying and Engaging with the Ethical Implications of ICTs

[18] B. C. Stahl, "Responsible research and innovation: the role of privacy in an emerging framework," Science and Public Policy, pp. 1-9, 2013]
[19] Steering Board of the European Cloud Partnership, Establishing a Trusted Cloud Europe – Final Report 2014

3.3 Policy Reflection Paper 3: RRI for Security

1. Executive Summary

The aim of this brief is to depict the current dimensions and challenges of surveillance technologies, as well as the potential benefits of integrating principles and approaches of RRI within research and technological development of surveillance systems for security. Moreover, this brief will depict two pillars that are part of the RRI concept which are impact assessment and public engagement in the development of such systems. The goal at the end is to generate recommendation for the improvement of mechanisms for ethics surrounding surveillance for the governance of surveillance technologies.

2. Notions of Security

"*Security is the condition (perceived or confirmed) of an individual, a community, an organization, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, [and] disasters (natural and man-made)"* [1].

At present security approaches have a very large and complex area of operation. These approaches do not only focus on the defence of the nation state's borders, but also, on protecting every human being [2]. The notion of security is perceived to encompass the broader concept of "securitization" which is generally associated with the Copenhagen school of security studies [3]. Securitization is a specific academic terminology used in the field of security which entails the transformation of subjects and incidents into a matter relevant enough, to enforce security measure mains by state [3]. This broader view of security holds that security is existentially linked to survival, and goes beyond military conceptions and "traditional" military security (defence). In the twenty first century, traditional focus on military state security perception has been broadened up to include a wider range of issues touching upon human life to be considered as security issues.

Security today encompasses civil security (fight against terrorism, protection and prevention against crime, prevention and detection of fraud, cyber security, energy security) in the face of geo-political threats to energy supplies and in the context of environmental concerns exacerbated by climate change), environmental security, food security (both in the context of food safety and food supply), health security (i.e. disease prevention and treatment) as well as social security.

In the contemporary global context, such dimensions of security are particularly salient in the context of urbanization and civil security. In practice, Perceptions of security between the state and the civilians also vary. These different perceptions are conditioned by several interpretations on relevant security principles or themes such as human security and personal security.

For example, it has been widely acknowledged that human security factors may include health, wellbeing, financial stability, welfare, civil liberties and human rights, as well as less tangible existential notions of home, place, freedom, respect and happiness. The concept of personal security, on the other hand, as explicitly emphasized in the Charter of Fundamental Rights and Freedoms, is about the protection of human rights that will require the state to take appropriate measures to safeguard these rights from violation by others (security measures as positive obligation of the State) [4]. These interpretations of security, for

example, are inarguably contributing to the differences on security perception and expectation from the viewpoints of individuals and the state. These discrepancies in the perceptions are widely perceived in an increasingly urbanized society. Since the state feels the security of an urban environment and thus its citizens can be established by a surveillance system installed in a public place for example, whereas such a system poses and evasion in the human security by restricting his freedom.

2.1 Challenges of urbanization

The trend of urbanization has posed great challenges to many municipal governments in dealing with providing sufficient security to all urban residents [5]. Although urbanization is not a new phenomenon, in the past few years, the unprecedented speed and scale of demographic shifts due to the trend has caused great security concerns. At the beginning of the 19th century, just about three percent of the world constituted an urban population [5]. In 1990, fewer than 4 in 10 people lived in urban areas. However, in 2010, the world urban population has increased more than ever before, and over half was noted to live in cities. By 2050, it has been speculated that the urban population could grow to 7 out of every 10 people. At the same time, the impact of adverse events such as contamination of the water supply, natural disasters or crimes is amplified in increasingly densely populated urban settings [6]. Further, the interconnectedness and agglomeration of infrastructures in urban areas, inarguably, are exposed to heightened risks of being attacked**.** Urban security as such has come to represent one of the most challenging problems of global security agenda

2.2 Civil security

Dependent on national context and usage, civil security may also be substituted by terms such as homeland security, national security or human security. It encompasses the protection of civilians against new threats and the resilience of technical systems as well as the functioning of important infrastructures. Citizens expect their governments to prepare for crises and disasters, to prevent critical events from happening as far as possible, to protect values and infrastructures from harm and to respond effectively when a crisis does occur [7].

In today's globalized world, societies and nations are facing on-going and emerging security problems that pose great challenges to deal with. These new security problems and challenges will require a systematic inquiry to re-examine the existing security concepts and measures. This process is fundamental in any effort to formulate viable security policies to effectively respond to future security challenges facing the society and its citizens. In the context of urbanized and networked societies for example, the new and emerging threats related to urban security impose challenges on communities to exercise security rights and to propose effective security measures. Due to the nature of the security risks associated with this modern way of living, one will argue that, if the safety and security of civilians, and their welfare, has traditionally been the responsibility of nation states, these states might no longer possess all of the means to deliver [8]. In the contemporary global context, the provision of public goods and security is also provided by other actors than the state. Many of these actors have been identified under the umbrella of transnational corporations and -governmental organisations and supranational and international institutions.

2.3 Surveillance in urban areas

As populations in cities are growing, traffic management, environmental problems and the security of citizens as well as critical infrastructures pose severe and growing challenges to policy makers and local administration. In response to such challenges, surveillance systems have been introduced as a security response to deter threats arising in urban cities. Since human surveillance involves high costs, cameras, which may be either preventive or dissuasive, are primarily watching over spaces dedicated to transport, public gathering, and shopping centres today [9]. Video surveillance systems have also been perceived as a useful tool to fight terror attacks, identify criminals, enhance the work of police and overall foster the perception of safety. Yet the use of surveillance systems is controversial and their effectiveness and legitimacy is subject to debate, although people's perception to these systems has changed as they got even in many cases indifferent to their existence and being daily exposed to them (habituation effects[1]). On the other hand, there is a huge disproportionality between the financial expenses and privacy costs of these systems in comparison with the actual a constructive contribution to the investigation of criminal offences. However, it can be argued, that the effects of surveillance in urban areas cannot be evaluated without a consideration of the specific technologic constellation, the consequences of a security breach, as well as environmental embedding under which a surveillance system is expected to work. Rather than generalizations about the nature, impact and extent of surveillance in urban agglomerations[2], surveillance should be assessed and implemented according to the concrete purpose of deployment, the level of technological sophistication, the accompanying operating procedures as well as personal staffing policies [29]. Hence, facilities and effects must be inevitably regarded as the outcome of a specific interaction and setting of organizational, cultural and technological variables.

Hundreds of cameras are producing countless images of people and public spaces every day which then have to be analysed and interpreted by trained personnel. Due to staffing shortages and a limited amount of time, there has been a massive increase in demand for smart surveillance systems which are capable of automatically detecting certain incidents such as left-behind baggage, offensive actions, crowds or people who moved too close to edge of a train platform. According to the article "Sorting out smart surveillance" written by Wright et al. 2010, smart surveillance is defined as "a system which is able to extract application-specific information from captured information to generate high-level event descriptions that may be used to make automated or semi-automated decisions" [10]. Advances in imaging algorithms facilitate the automated operation of surveillance systems, thus, relieving the operators of the task of manually monitoring video footage. Computerised systems for automated face recognition, gait recognition and complex activity recognition can continuously scan hundreds of video streams and direct the attention of human operators only to critical events [10].

Other devices, including mobile and smart phones, PDAs, satellite navigation systems, which all depend on GPS systems as well as Radio Frequency Identification (RFID), allow for new forms of monitoring. Surveillance need no longer be limited to a particular geographical

[1] **Habituation** is a decrease in response to a stimulus after repeated presentations.

[2] Densely populated urban areas

space. Unlike CCTV which continues to focus primarily on specifically defined locations, monitoring associated with devices such as GPS and RFID is neither restricted to any interior and architectural space, nor does it depend on human observation in order to function [11]. The term "smart city" for instance refers to a trend that influences a number of IT-driven public policies dealing with the key infrastructural networks of urban areas, from motorways to electricity grids and from water pipelines to public transport. IBM has launched a "Smarter cities" programme which covers a wide range of interconnected places and phenomena, such as policing, city administration, mobility, energy management and consumption monitoring. These efforts work through global communication networks and inter- and intra-urban mobility control techniques like border controls, GPS and other location and tracking technologies [12].

3. RRI and Surveillance

Technological development, enhanced communication networks and a smarter deployment of CCTV, for instance the usage of facial as well as behavioural pattern recognition, enables a significantly more comprehensive surveillance of citizens in public space areas, thus triggering a number of fundamental rights and privacy issues. Besides the cost that may be produced by surveillance technologies, the implications of CCTV such as privacy impact, effectiveness and social consequences are points of criticism [13].

In this context, surveillance technologies should not only be deemed as a neutral mean mobilized by actors to deal with perceived problems or needs. Surveillance technologies should also have the ability to adapt to the differences in an urban environment and learn from personal knowledge, experience, and relationships in a social system [14][15]. Effects and experiences of surveillance differ by population, purpose, and setting. Surveillance systems obtain personal and group data in order to classify people and populations according to varying criteria, to determine who should be targeted for special treatment, suspicion, eligibility, inclusion, access, and so on [16]. Such social sorting indicates the tendency for surveillance systems to operate as mechanisms for societal differentiation. Surveillance systems actively construct differences among populations and regulate those populations according to their assigned status. In this regard, surveillance technologies are never impartial. Surveillance systems such as CCTV on airports, for example, are tools of societal differentiation and may establish or sustain social inequalities. While defining high-risk groups, screening for potential dangerous people (according to race, class, gender, age, etc.), they serve to diagnose peoples "appropriate" outward appearance and behaviour, manifested and inscribed in the technological processes (such as search algorithms) underlying surveillance systems [15]. In this context, the problematic impetus is twofold: first it pressures people not to diverge from assigned categories, thereby reinforcing existing social divisions or creating new yet invisible hierarchies of access and privilege. For instance, facial and behavioural pattern recognition encloses critical presumptions on specific pattern of human behaviour and outward appearance that are closely linked to existing societal stereotypes and preconceptions.

Surveillance as a security tool, in this regard is always ambiguous and its ethical implications are hard to grasp. On the one hand, a feeling of security appears to be a necessity for human development. On the other hand, concerns about security can be used to enforce potentially problematic power relationships. Hence, security can be seen as an ethically problematic mechanism of domination [17]. Privacy is a central notion in the ethical debate on

surveillance and security. Privacy means the right to protect actions and thoughts that persons want to keep to themselves. It refers to the state of being separated, secluded from others, in contrast to the state of being public or common [4]. Discourses about surveillance and security most commonly argue with regard to mistaken trade-offs, often between security and privacy. This framing unreflectively implies that surveillance (technologies) work as intended, assuming that people are able to make rational choices about adopting surveillance or disclosing themselves to it, as well. Moreover it is presented as if surveillance does not create new insecurities or problematic effects.

However, in everyday life, people are just not in the position to choose, but rather have to accept the inevitable, whether for justifications of crime prevention, state's security or employee monitoring. On the other hand, Scholars have found that the mere presence of CCTV can cause fear in people who strictly relate the presence of surveillance as the existence of an eminent danger, which in turn affects the way people behave and feel comfortable [28]. Moreover, video surveillance exerts power through its very asymmetric nature: while one is surveyed by someone (consciously or not), there is no way for a reciprocal look back, nor information about from whom one is surveyed. The increase of voyeuristic recording of women by men, where women becoming subject of harassment, whether in official control spaces or with smartphone cameras in public space, is one example of an unanticipated effect of surveillance. Social space becoming increasingly hostile in this context obviously counteracts anticipated results of increasing safety and security [28].

One approach to address the ambiguities and ethical impacts inherently linked with surveillance is the relatively new concept of responsible research and innovation (RRI).RRI focuses on the time frame between the initial phases of research strategy formulation and the point at which individuals and organizations use products and services based on research output. The key component of RRI is the development of greater democratic accountability within the innovation lifecycle [17]. The concept of RRI also includes an inter- and transdisciplinary approach. Projects bring together actors from industry, civil society and research to ensure a more responsive, adaptive and integrated management of the innovation process. Additionally RRI encourages an on-going public debate and urges to monitor and harness public opinion. This opinion is essential for the legitimacy of research funding and particular scientific and technological advance [18].

3.1 RRI - Ethical and societal impacts of security research

Many surveillance practices have a direct effect on the nature of the society in which they are embedded, in terms of categorical discrimination and social exclusion [20]. Security impacts can be powerful, and are often distributed unevenly across society. Some groups are more vulnerable to the negative effects of security research and implementation and are often excluded from decision-making processes. Surveillance systems such as in transportation systems, urban infrastructures and identification documents substantially modulate people's experience of the world. It is not least this extensive consequence that makes surveillance systems a considerably relevant subject to RRI. Similar to legislation, research and technological development of surveillance systems shape social practices in a normative way. Technologically provided sets of rules (algorithms) encourage certain ways of interaction and usability while constraining others. For instance, CCTV manifests the remote observation of people, as much as walls and boundaries manifest a demarcation of

belonging. The emphasis of the agential character of surveillance technologies does not follow a simplistic notion of technological determinism, nor does it deny the agency of people. Rather, the agential power exerted upon people must become reflected and made transparent. It is exactly this technological framing of what is amenable and practical, for individuals as well as organizations, which implies the political dimension of surveillance technologies. This is in particular critical in the light of decisions on concrete implementation of technologies: Only rarely there are subject to public discourse and democratically legitimized decisions. RRI in surveillance therefore provides a valuable basis for opening up for societal discourse and the controversies regarding the constitutive role of surveillance systems, with respect to the analysis of social insecurities and inequalities,

Additionally, security research has often less transparency than in areas where national interests are not seen as affected in such an immediate way. Therefore, it is important to consider the wide range of possible societal impacts of research activities by increasing the reflexivity of the research process. Reflexivity means here the ability of researchers to take stock of their role in the research process and subject their research to critical scrutiny [21].

RRI is based on normative guidelines and recommendations that encompass human rights, internationally binding treaties and philosophical ethics, which are accepted principles that are sufficiently defined to provide the basis for collective action [17]. The Societal Impact Expert Group highlights the importance of research ethics, citizens' rights and societal relevance. Research ethics refers to a common set of norms and principles including the accountability for scientific procedures, disinterestedness, regard for conflict of interest, consent of participants in research, confidentiality, transparency of methods, among other things. Societal relevance asks whether research actually leads to enhancing the security of European citizens and how it will affect the lives of citizens in doing so. However, citizens' rights should be a fundamental criterion to distinguish what is, and what is not acceptable in security research [19]. Impact assessment and public participation are at the core of RRI and may serve to meet the ambivalent implications of surveillance for security.

3.2 RRI - Impact assessment and public engagement

As surveillance systems may raise risks for individuals as well as society, impact assessment as part of RRI should aim at assessing the risks of surveillance-related projects, policies, programmes, or products. In spite of the prevalence of surveillance in the urban society, it is surprising that no one has yet developed a method for assessing the impact of surveillance on society. One reason is that regulators, privacy advocates and academics have felt that a privacy impact assessment (PIA) is sufficient for identifying and analysing the impacts of surveillance [31]. While privacy and data protection are an important part of the assessment, surveillance affects a range of other fundamental rights. Hence, ethical and social principles should also be included in the assessment process [22]. Assessment also requires cost/benefit analysis between the different courses of action and the different values at stake. However, the aim of such balancing is not to weight one fundamental right against another but to reconcile the multiple values that constitute the backbone of the democratic State [24].

Public engagement complements assessment activities by engaging users and civil society organisations on all levels of the RRI process. It endures regretfully allot of deficits, since the general conception by stakeholders from security field is that, the knowledge from the public is inferior to that held by apparent expert [30], although public consultations may

contribute to the formulation of the research agenda as well as to the research and innovation activities itself, but it may also be conducive to the dissemination of research outcomes. Engage2020 is an example of an EC funded project that aims to increase the use of engagement methods and policies in research and innovation. The project also aims to map and explore what is practiced and by inspiring researchers, policy makers and other interested parties[3]. Such a project aims to create methods and tools for public engagement that will accompany any project including security projects that will take part of Horizon 2020.

It is clear that the EU along other international actors have realized that by making use of the knowledge of civil society, research and innovation process can be organized in a more targeted and effective way. Furthermore, it raises public acceptance of products and outcomes. Likewise, decisions with regard to research and innovation need to include societal interests and values to be perceived as legitimate [23]. Since science is potentially political, public deliberation and representation is required to legitimate its outcomes in a democratic way [25].

3.3 The challenge of participation in security research

In some instances states and organizations have a legitimate interest in keeping security issues confidential. Thus, RRI in security research has to address questions of transparency, inclusiveness and accountability, reducing thereby the secretiveness of security programs where possible. Participatory procedures may strengthen security research projects by broadening the basis of knowledge and of the values involved. Also, participatory approaches help to realise common interests and increase the acceptance as well as the legitimacy of a decision [26]. Participation may introduce new perspectives and insights into the research process – but only if information is shared and communicated as much as possible and necessary to relevant stakeholders. By involving a variety of stakeholders, an increased amount of potential risks will be highlighted and risk management becomes possible. Additionally, individuals, groups and organisations should have the opportunity to identify themselves as stakeholders and request participation [27]. Participation does not only encompass the expression of opinions and differing positions. Participative methods also facilitate the exertion of influence on the decision-making process.

4. Conclusion and Recommendations

Taking into account the dimensions and challenges of surveillance technologies outlined above, as well as the potential benefits of integrating principles and approaches of RRI within research and technological development of surveillance systems for security, some concluding recommendations can be drawn.

- RRI is one approach to address the ambiguities and ethical impacts inherently linked with surveillance. RRI strengthens security research projects by broadening the basis of knowledge and of the values involved. In particular, participatory approaches help to realise common interests and increase the acceptance as well as the legitimacy of political decision making.

[3] http://engage2020.eu

- At its core, RRI promotes activities to embed openness and *transparency* in the research and technological development process. This becomes especially important with regard to emerging technology's governance. As emphasized above, the reduction of secretiveness of security programs where possible, is of utmost importance. Only through the courageous inclusion of a variety of stakeholders, all potential risks will be highlighted and risk management becomes possible. This serves not only norms, but also functional purposes for political decisions to become robust.
- It is important to consider the wide range of possible societal impacts of research activities by increasing the reflexivity of the research process. Reflexivity means here the ability of researchers to take stock of their role in the research process and subject their research to critical scrutiny.
- One significant element is the surveillance and privacy impact assessment as part of RRI. As surveillance systems may raise risks for individuals as well as society, the impact assessment promotes the assessment and monitoring of risks of surveillance-related projects, policies, programmes, or products. Risk assessment addresses the likelihood of a certain event and its consequences proactively. Assessment also addresses the impacts of research activities by increasing the reflexivity of the research process. Hence, RRI is a valuable tool for decision makers to further sensitize complex issues.
- All assessment activities need to be informed by different social perspectives and interests. Conclusions are not only determined by pure scientific data but are the result of interpretations which depend on different values and different scientific paradigms and theories. The particular knowledge of those affected by technology implementation has to be made available, in order to describe properly the chances and risks connected with the technology at stake and to define possible solutions [23]. The assessment should include all relevant stakeholder and be conducted throughout the life cycle of a surveillance initiative.
- Building Confidence is crucial, both for technology developers and society at large. Therefore it should become mandatory in development projects for surveillance systems, first to explore what stakeholders - including ordinary citizens, since they form the largest affected group - expect, and how research and companies can respond. This also lies in the core of the RRI principle to avert unwanted consequences.
- The development of technology moves forward with increasing pace. Strong impact assessment as well as inclusive participatory collaboration on project level for security research and development across Europe should be encouraged and supported (e.g. in reference to requirements in calls, funding schemes).

Bibliography

[1] J. Sieber (Institute for the Protection and Security of the Citizens - IPSC), "Presentation on CEN BT/WG 161 - Standards for Security and Protection of the Citizens," in Security Research Conference, Ankara, 2008.

[2] European Commission, "Ethical and Regulatory Challenges to Science and Research Policy at the Global Level," D.G. for Research and Innovation, Brussels, 2012.

[3] Buzan, O. Weaver and J. de Wilde, Security: A New Framework for Analysis, 1998.

[4] European Group on Ethics in Science and New Technologies to the European Commission, Ethics of security and surveillance technologies - Opinion no. 28, 2014.

[5] Canadian Consortium on Human Security and Human Security Research and Outreach Programme of Foreign Affairs and International Trade Canada, “Human Security for an Urban Century. Local Challenges, Global Perspectives,” 2007.
[6] World Health Organization / United Nations Human Settlements Programme, “Executive Summary. Hidden cities - Unmasking and Overcoming Health Inequities in Urban Settings,” 2010.
[7] UI papers no. 2, “Civil Security and the European Union: A survey of European civil security systems and the role of the EU in building shared crisis management capacities,” Swedish Institute of International Affairs, 2014.
[8] R. McRae, “Human Security in a Globalized World,” in Human Security and the new Diplomacy. Protecting People, Promoting Peace, Québec, McGill-Queen's University Press, p. 17, 2001
[9] Eurpean Forum for Urban Security, “Citizens, Cities and Video Surveillance - Towards a democratic and responsible use of CCTV,” 2010.
[10] Wright et al., “Sorting out smart surveillance,” Computer Law & Security, vol. 26, no. 4, pp. 343-354, 2010.
[11] L. Muir, “Control Space? Cinematic Representations of Surveillance Space Between Discipline and Control,” Surveillance & Society, vol. 9, no. 3, pp. 263-279, 2012.
[12] F. Klauser and A. Albrechtslund, “From self-tracking to smart urban infrastructures: Towards an interdisciplinary research agenda on Big Data,” Surveillance & Society, vol. 12, no. 2, pp. 273-286, 2014.
[13] SurPRISE, “D 3.1 - Report on surveillance technology and privacy enhancing design,” 2013. [Online]. Available: http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE-D3.1-Report-on-surveillance-technology-and-privacy-enhancing-design.pdf. [Accessed 1 December 2014].
[14] T. Monahan, “Surveillance as cultural practice,” The Sociological Quarterly, vol. 52, pp. 495-508, 2011.
[15] T. Monahan, “Editorial: Surveillance and Inequality,” Surveillance & Society, vol. 5, no. 3, pp. 217-226, 2008.
[16] Lyon, “Surveillance as social sorting,” in Surveillance as Social Sorting - Privacy, risk, and digital discrimination, Routledge, 2003, pp. 13-30.
[17] B. Stahl, G. Eden, M. Jirotka and M. Coeckelbergh, “From computer ethics to responsible research and innovation in ICT - The transition of reference discourses informing ethics-related research in information systems,” Information & Management, no. 51, pp. 810-818, 2014.
[18] R. Von Schomberg, “Prospects for Technology Assessment in a framework of responsible research and innovation,” in Technikfolgen abschätzen lehren: Bildungspotenziale transdisziplinärer Methoden, Dusseldorp and Beecroft, Eds., Wiesbaden, VS Verlag, 2012, pp. 39-61.
[19] Societal Impact Expert Working Group, “Report of the Societal Impact Expert Working Group - EC DG ENTR Report,” 2012. [Online]. Available: http://cies.ie/wp-content/uploads/2014/05/Report-of-the-Societal-Impact-Expert-Working-Group.pdf. [Accessed 10 12 2014].
[20] Surveillance Studies Network, “A report on the surveillance society. For the Information Commissioner by the Surveillance Studies Network,” 2006. [Online]. Available: http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/02_11_06_surveillance.pdf. [Accessed 11 12 2014].

[21] K. Wadhwa, D. Barnard-Wills and D. Wright, “The state of the art in societal impact assessment for security research,” Science and Public Policy, pp. 1-16, 2014.
[22] SAPIENT, “Deliverable 4.4: A guide to surveillance impact assessment - How to identify and prioritise risks arising from surveillance systems,” 2014. [Online]. Available: http://www.sapientproject.eu/D4.4%20-%20SIA%20Manual%20%28submitted%2001%20August%202014%29.pdf. [Accessed 15 12 2014].
[23] L. Hennen and S. Pfersdorf, “Public Engagement - Promises, demands and fields of practice - Deliverable 2.1 of the project Engage 2020,” 2014.
[24] Wright, R. Gellert, S. Gutwirth and M. Friedewald, “Precaution and privacy impact assessment as modes towards risk governance,” in Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields, 2011, pp. 83-98.
[25] M. Brown, Science in Democracy - Expertise, Institutions and Representation, MIT Press, 2009.
[26] Bora and H. Hausendorf, “Participatory science governance revisited: normative expectations versus empirical evidence,” Science and Public Policy, vol. 33, no. 7, pp. 478-488, 2006.
[27] Assert, “Toolkit for Societal Impact Assessment in Security Research - Report on Deliverable 3.2,” 2014.
[28] T. Monahan, “Surveillance in the time of insecurity”, Rutgers university press, 2010
[29] L. Hempel, and E. Topfer, “CCTV in Europe”, Final Report, The Urbaneye Working Papers Series, edited by 5th Framework Programme of the European Commission, 2004
[30] Goold, B. J.; Neyland, Daniel, “New directions in surveillance and privacy”. Cullompton, Devon, U.K., 2009
[31] David Wright, Charles D. Raab, “Constructing a surveillance impact assessment, Computer Law & Security Review”, Volume 28, Issue 6, December 2012, Pages 613-626

3.4 Industry Reflection Paper 1: RRI Approach in Engaging Stakeholders for Sustainable Palm Oil in Malaysia

1. Executive Summary

Global palm oil production is dominated by Indonesia and Malaysia, where the total production of palm oil from these countries has yielded about 86% of world production of palm oil for this sector in 2013. In 2014, respectively, 46% and 41% of palm oil yield were from Indonesia and Malaysia. Although Palm oil is a very productive crop the global production of and demand for palm oil is increasing rapidly. Plantations are spreading across Asia, Africa and Latin America. But such expansion comes at the expense of tropical forests—which form critical habitats for many endangered species and a lifeline for some human communities. Reflecting on the on-going challenges facing the Malaysian palm oil industry, this brief aims to highlight the benefits of integrating principles and approaches of Responsible Research and Innovation (RRI) to the industry in order to achieve a more ecologically sustainable and societally acceptable industry.

2. Problem Description

2.1 Statement of the current industrial state

Grown only in the tropics, the oil palm tree produces high-quality oil used primarily for cooking in developing countries. It is also used in food products, detergents, cosmetics and, to a small extent, biofuel.

Global palm oil production is dominated by Indonesia and Malaysia, where the total production of palm oil from these countries has yielded about 86% of world production of palm oil for this sector in 2013. In 2014, respectively, 46% and 41% of palm oil yield were from Indonesia and Malaysia. Other countries, that include Thailand, Colombia and Nigeria, contributed to the remaining market share. Countries such as India, China, those within the European Union (EU), Pakistan, USA, Vietnam and Japan are noted as among the top importers for palm oil. In Europe, there is a growing demand from the EU countries for the oil to be used in producing biodiesel. Palm oil is a cheaper alternative source of raw material that can replace rapeseed and sunflower oils for the biodiesel industry, in which currently is leading by the EU. The increasing demand for palm oil in relation to biodiesel production offers strategic opportunity for major exporters of palm oil such as Malaysia to develop local biofuel industry and technology. Malaysia aims to produce and export biofuel, and is targeting to penetrate the EU market in the near future.

In Malaysia, the oil palm industry contributes around 5-6% of the country's GDP. At present, palm oil products from the industry can be categorized in four broad categories, namely: (1) palm oil and palm kernel oil products; (2) oleochemicals; (3) biodiesel; and (4) palm biomass product. With regard to oil palm cultivation areas, the two Malaysian states located at the Borneo region – Sabah and Sarawak – recorded the largest cultivation areas for palm oil. Sabah recorded about 28% of total oil palm planted area, whilst Sarawak recorded about 23% of total cultivation area for oil palm in Malaysia. Peninsular Malaysia accounted for the remaining 49% of total oil palm planted area.

2.2 Statement of the problem

Palm oil is a very productive crop. It offers a far greater yield at a lower cost of production than other vegetable oils, but global production of and demand for palm oil is increasing rapidly. Plantations are spreading across Asia, Africa and Latin America. But such expansion comes at the expense of tropical forests—which form critical habitats for many endangered species and a lifeline for some human communities. This increasing rate of demand has caused the expansion of palm oil cultivation areas is claimed to contribute to deforestation, in which have direct ecological effects on biodiversity. Because of this contention, there have been on-going criticisms and campaigns by local and international non-governmental organisations (NGOs) towards the Malaysian palm oil industry. The biodiversity loss including the displacement of Orang Utans at the Borneo region due to deforestation has received wide attention from the global stakeholders from industry including certain consumer segments of palm oil products. The wide publicity received from the campaigns particularly in the European region has affected the Malaysian palm oil industry including the small farmers.

3. Industrial measures

3.1 Overview of the current global measures

Several Malaysian industry players have jointly participated in establishing Roundtable on Sustainable Palm Oil or RSPO. RSPO consists of various industry stakeholders - palm oil growers, palm oil processors and traders, environmental NGOs, social NGOs, consumer goods manufacturers, bank/investors, and retailers – that has a mission to influence the industry worldwide supply chain to promote sustainable palm oil cultivation. RSPO established an international certification system with regard to sustainability practices in the oil palm supply chains[4]. RSPO certification is crucial for exporting palm oil products targeted for European and other Western's markets. RSPO upholds eight principles in promoting the practice of sustainable palm oil. The principles are: (1) commitment to transparency; (2) compliance with applicable laws and regulations; (3) commitment to long-term economic and financial viability; (4) use of appropriate best practices by growers and millers; (5) environmental responsibility and conservation of natural resources and biodiversity; (6) responsible consideration of employees, and of individuals and communities affected by growers and mills; (7) responsible development of new plantings; and (8) commitment to continuous improvement in key areas of activity[5]. RSPO, however, has been accused by several palm oil players as being dominated by influence from the NGOs such as Western activists and World Wildlife Fund (WWF)-related individuals at various governance levels and structure of the RSPO[6]. This concern, among others, has led the Malaysian Palm Oil Association (MPOA) to reconsider quitting from RSPO group. At the moment, the RSPO has reached more than 2,500 members for various palm oil producing countries, out of which over 120 members are from Malaysia. The RSPO has developed 300 Trademark license for the produced palm oil by the participating members.

[4] Wild Asia, 2012 - oilpalm.wildasia.org

[5] http://www.rspo.org/

[6] http://www.thestar.com.my/Business/Business-News/2014/02/26/Malaysian-Palm-Oil-Association-to-announce-decision-on-Friday/?style=biz

Since there is in an ever-urgent need and growing global concern that commodities are produced without causing harm to the environment or society. RSPO certification is an assurance to the customer that the standard of palm oil production is sustainable. Palm oil producers are certified through strict verification of the production process to the stringent RSPO Principles & Criteria for Sustainable Palm Oil Production by accredited Certifying Bodies, and can be withdrawn at any time in case of infringement of the rules and standards. All organisations in the supply chain that use RSPO certified sustainable oil products are audited to prevent overselling and mixing palm oil with conventional (or non-sustainable) oil palm products. These organisations can claim the use of RSPO certified sustainable oil palm products "on pack" by using the RSPO Trademark.

3.2 Overview of the current Malaysian measures

The Malaysian government and agencies (federal and state level) have effectively responded in addressing the international concerns, and simultaneously also, have undertaken serious efforts to protect the image of palm oil and to advance the palm oil industry including the implementation of various sustainability programs and support incentives for oil palm R&D and innovation activities . The practice of sustainable palm oil in the industry is one of the crucial initiatives to reduce deforestation and to strengthen conservation efforts to protect biodiversity.

Whilst various systematic efforts being introduced to innovate the industry practice and standards, yet it is not known to what extent these efforts have reached the wider stakeholders such as small farmers to educate and facilitate them regarding sustainable palm oil practices, and what role can they play as small farmers to contribute to the conservation efforts to protect biodiversity. In Malaysia, at present, there are more than 300,000 small farmers in the palm oil industry. Small farmers represent close to 40% of palm oil cultivation area in Malaysia.

In the Malaysian context, two important government institutions that have important roles in the industry are the Malaysian Palm Oil Board (MPOB) and the Malaysian Palm Oil Council (MPOC). MPOB (http://www.mpob.gov.my) play roles to advance the palm oil industry via R&D and innovation related activities; MPOC (http://www.mpoc.org.my/) involves in promoting and expanding the industry for the global market. MPOC established Malaysian Palm Oil Wildlife Conservation Fund (MPOWCF) as part of a systematic effort to conserve and protect biodiversity including Orang Utan. In addition, the two biggest states – Sabah and Sarawak – that produce high oil palm yield are also collaborating and cooperating with WWF-Malaysia to reduce deforestation and enhance conservation efforts[7]. Malaysia further established Malaysian Sustainable Palm Oil (MSPO) standard as a national standard for certification scheme to certify on sustainability practices (including premises) that abide Malaysian laws and international agreements[8]. MSPO is applicable to small, medium and large industry players in the sector, and is just implemented this year. MSPO is the third

[7] http://www.wwf.org.my/?19485/Reducing-deforestation-in-Malaysias-Bornean-states-of-Sarawak--Sabah

[8] http://www.mpoc.org.my/upload/IPOSC-2014-Malaysian-Sustainable-Palm-Oil-Current-Status-Dr-Ainie-Kuntom.pdf

certification scheme standard in the world for palm oil, after the ISPO (Indonesian Sustainable Palm Oil) that was launched in 2011, and the RSPO that was set up on 2004[9].

3.3 Argument for why and how current action is failing

The measures that have been done are still not efficient enough since a country like Malaysia have a big part of its economy reliant of this natural resource, and the industry with the assistance of the government has to comply with this increasing demand in order to insure the economic stability of the company and country alike. The eternal confrontation between the top down government and industry approach to the bottom up environmental NGO leads to the delay of feasible solutions towards an actual sustainable palm oil industry.

Sustainable palm oil has been under fire for several years from environmentalists and organisations who feel it is nothing more than a greenwashing scheme. This view did not improve within the environmental community upon the formation of the RSPO (Roundtable on Sustainable Palm Oil) in 2004, but many feel that this widely accepted certification scheme has the potential to prevent deforestation in the industry. The RSPO aims to unite stakeholders form all sectors of the palm oil industry, including environmental and social NGOs. But although the RSPO is currently the largest sustainability-focused organisation within the palm oil sector, its standards do not ban deforestation or destruction of peatlands for the development of oil palm plantations. Although most of the prominent companies dependent on palm oil have joined the RSPO and also raising concerns towards the deforestation and negative effects, this demand has not dropped and they continue to consume palm oil in the regular rates leaving their commitment in form of this raised concern.

4. Industrial Recommendations and Conclusions

The core of Responsible Research and Innovation (RRI) is the integration of responsibility awareness in all aspects of production and especially innovation. A big part of this responsibility is towards the society and nature which can be established by working towards a sustainable palm oil industry which is an approach to oil palm agriculture that aims to produce palm oil without causing deforestation or harming people.

Reflecting on the on-going challenges facing the Malaysian palm oil industry, the following are the highlighted benefits of integrating principles and approaches of Responsible Research and Innovation (RRI) to the industry.

- RRI promotes reflexivity, and this can be an effective tool for decision makers.
- RRI encourages innovative solutions by bringing wider stakeholders' viewpoints and concerns as feeder to the reflexive process undertaken to attain best decisions.
- A dialogue has to be initiated,
- RRI includes global stakeholder participation as it promotes shared responsibility and accountability.
- RRI aims to set tools for collaboration by which various stakeholders can use to promote opinions and reach common understanding towards the effective sustainability of palm oil.

[9] http://www.thejakartapost.com/news/2015/03/02/newly-implemented-malaysian-sustainable-palm-oil-means-more-business.html

- RRI also aims to assist industries in their innovation by including the various societal aspects into that process, which would lead to products, cultivation methods that are ecologically compliant and societally acceptable.
- RRI is based on the principle of open interaction, engagement and transparency to approach a problem. Hence RRI is a valuable tool for decision makers to further sensitize complex issues.

Bibliography

[1] RSPO - http://www.rspo.org/about/impacts

[2] SSI Review 2014 - https://www.iisd.org/pdf/2014/ssi_2014_chapter_11.pdf

[3] Chin, 2011 - http://www.cifor.org/publications/pdf_files/WPapers/WP64CIFOR.pdf

[4] MPOB, Jan 2015 – Overview of the Malaysian Oil Palm Industry 2014 [http://pmspk.moe.gov.my/wa/wp/wawp.php?proxy_url=aHR0cDovL2JlcGkubXBvYi5nb3YubXkvaW1hZ2VzL292ZXJ2aWV3L092ZXJ2aWV3X29mX0luZHVzdHJ5XzIwMTQucGRm]

[5] Chapter 15 – the Malaysian Palm Oil Industry: Development and Challenges, 2007, page 372 – 373.

[6] MPOB, Jan 2015 – Overview of the Malaysian Oil Palm Industry 2014

4 Conclusion

Through this deliverable we have outlined the importance of, production of, and the versions of the four reflection papers that were produced as part of RESPONSIBILITY. In each case we provide recommendations surrounding the four subject areas of choice. These show the importance and necessity of embedding an RRI-oriented approach to respond to and deal with particular or potential problematic issues. Importantly, the papers are seen as important tools in bridging the gap between research outcomes, and policy/industry activities.

There are a number of directions the future development of the reflection papers may take. Initially it is foreseen that they would be added to the corpus of materials within the Observatory, providing an important tool in engaging with the wider stakeholder community in relation to the diffusion and dissemination of RRI. It may also be that the papers themselves could be used to inform more substantial policy reflexions that can then be formally released to either policy makers or industry.

Importantly, it is seen that the papers can act as a tool for these wider stakeholder communities to engage with the importance of embedding RRI within their practices, procedures and products. We see the importance of aligning research and innovation practice and outcomes to societal needs, as the principles of RRI denote, encouraging anticipation of and mitigation of potentially or existing harmful issues.