Legislative Tensions in Participation and Privacy

Michael Boniface, Brian Pickering

University of Southampton IT Innovation Centre (mjb@it-innovation.soton.ac.uk)

Eric Meyer, Cristobal Cobo

Oxford Internet Institute (eric.meyer@oii.ox.ac.uk)

www.seserv.org

© University of Southampton IT Innovation and Oxford Internet Institute 2011

Table of Contents

1 Executive Summary

Two-thirds of the world's Internet population now visit an online community or blogging site and the sector now accounts for almost 10% of all Internet time. A quarter of a million users sign up to social networking sites every day worldwide and a third of those who have a profile on a social network update it daily. Participation and privacy are critical success factors that underpin healthy and vibrant online communities. It is essential that Future Internet researchers understand the complexities of participation and privacy in the design of systems to ensure that technologies are socially, ethically and legally acceptable.

This report explores perspectives on participation and privacy within online communities by applying different analytical techniques to a case study from e-Government.

- **Collaborative network organisations (CNO)**: Design from the users' perspective
- **Tussles**: Design the playing field and not the outcome
- **Risk management**: Design for outcome considering uncertainty

In addition to discussing participation and privacy issues, each technique was assessed against the ability to 1) *construct issues and research challenges, 2) facilitate communication and debate, 3) assessment of technology advances, 4) improve engineering design through insights from other domains, 5) design legally compliant Future Internet systems and 6) improve project design and decision making*. The overarching conclusion was that examining the issues from different perspectives highlights different concerns that need to be considered within system requirements and architectural design. CNO highlighted the need for mechanisms to facilitate federation between different collaboration structures, tussles highlighted issues such as the economic conflicts in outsourcing processing of personal data to clouds and risk management identified the security mechanisms necessary for data protection compliance.

From a participation and privacy perspective the results showed that the goal to increase participation in political discourse through the use of popular social networking sites has many attractions. Likewise, the goal to comply with data protection legislation is also equally valid and as well as necessary. The CNO analysis shows that a critical success factor (i.e. participation) for social networking providers is to maximise activity, which is achieved irrespective of the purpose of the communication between individuals. The risk assessment highlights that for legal compliance providers must take responsibilities (in respect to purpose) and individuals need to take certain actions (e.g. consent). So here lies the contradiction. Privacy compliance, often declared as a way to increase trust, and hence participation, often impedes activity and actually acts as an inhibiter to participation in many situations. In reality, individuals use social networking sites because their perception of risk is considered low enough for participation. It is the perception of and appetite for risk that that dictate levels of participation, irrespective of associated regulation. Data protection can help but usually where low-levels of trust exist.

This leads to an interesting challenge for European service providers and research projects. How to balance strike the balance between participation and privacy considering desires to monitor and mine data without violating a citizen's right to privacy? Architectures that facilitate communication

between individuals regardless of purpose have been important innovators in the Internet. It is a principle that has contributed to the explosion of Internet use (the end-point principle) and it is improbable that the successful paradigms of the last decade, social networking and clouds, would not have prospered if they had considered compliance to the European regulatory environment. Each new paradigm has focused on promoting the benefits of solutions and opted for weak privacy positions. The try it and observe approach has allowed for a privacy balance to evolve over time as participants explored their preferences rather than having them analysed in advance by security experts. Social networking has been in fact a large experiment in people's appetite for privacy but how Europe strikes the balance between participation and privacy remains a matter of serious debate.

2 Introduction

Since its inception, the Internet has rapidly and without particular regulation or control become pervasive. What began as a fairly esoteric communication mechanism between academics has now become the *de facto* standard to complement or even replace traditional activities from banking and shopping to social interaction and information retrieval. The social aspects that affect the Internet and its evolution are as complex and interwoven as society itself. The interdependence of the analytical disciplines creates complexity, disciplines that study changes in human nature, where economics, political science, humanities, psychology and law are linked to concepts like privacy, freedom of expression, intellectual property and social networks but also to topics like education, security, regulation, private life, communication, business, trust, intangible incentives, to name but a few. What is clear is that creating teams that can be innovative through the development of novel Future Internet technologies is a complex endeavour.

The "real world" users of the Internet (i.e. consumers, citizens, students, politicians, scholars, artists, parents, etc.) constitute a powerful but also dynamic organism. Understanding the dynamics of individual and community behaviour, regulatory environments and markets and how such forces influence technical choices is increasingly important at all phases in the innovation lifecycle[1]. From early stage prototypes within university testbeds through to advanced pilots deployed within online communities or living labs, the needs and the rights of the stakeholders matter, and as the maturity of technology evolves they matter more. The challenge is to facilitate communication between different stakeholders and domains of expertise so that values can be debated, major issues can be constructed and the wealth of insights from the social science studies can be brought to bear on engineering decisions. Of course, as with most aspects of life, things are not that simple and such a dialogue must be approached from a broad and holistic perspective that acknowledges that each domain brings different viewpoints, languages and concerns. This is where ICT SESERV (http://www.seserv.org) comes into play by providing a multidisciplinary team that aims to bridge the gap between socio-economic experts and technologists. SESERV takes no specific position on technology, society or the economy but aims to act as a channel between disciplines. SESERV will engage with representative Future Internet projects to study socio-economic tensions and how they are addressed by project teams.

In this paper, we give a flavour of a multidisciplinary dialogue by examining one ICT project, *WeGov*. The project aims to make use of online communities as a way to increase the engagement of individuals and communities in government policy dialogue and debate. ICT research and development is at the heart of the project but evaluation of results through experiments and the freedom to use the results beyond the lifetime of the project are essential elements. The project must achieve data protection compliance for Future Internet research experiments that aim to collect and process personal data from online communities for the identification and tracking of political opinion whilst considering incentive models for individual participation in experiments: a challenge for a "Specific Targeted Research Project", which by its nature has a significant degree of risk and low maturity of technology[2]. The approach presented below focuses on the use and

[1] As the technology and the tools it creates become ever more powerful, so it is crucial for users to be made aware of the restrictions imposed on them and the incentives not to abuse them.

[2] To a significant extent, the *WeGov* project could be said to hold much responsibility. Beyond its own experiments, it must demonstrate that these data can be used fairly and legally. With this in mind, one of the deliverables is a code of conduct for those using the tools.

comparison of analytical methods from different domains as a way to provide socio-economic perspectives on the issues concerned: data privacy legislation and participation models.

3 The ICT *WeGov* Case Study

Governments have seen the value of the Internet to encourage public participation in policy planning and policy making. ***The challenge is how to motivate them***. Engaging citizens in Government, especially policy making and review, is not easy: there may be a lack of trust or simply no motivation to become involved, unless of course there is some feedback mechanism from those interested in the views expressed. Perhaps those who do tend to have rather polarised and non-representative views. One issue is the expectation of how participation might be reflected in the policies that are made: if the public perceive that their discussion is not taken into account in favour of the views or recommendations of experts employed directly by the Government[3], then involving the general public in government is bound to fail. One possibility is to try to capitalise on existing participatory fora: social networks. It is already known that online communities continue to flourish, irrespective of issues around privacy and data access. More importantly, participation within an appropriate institutional or organisational context can and does promote participation [14].

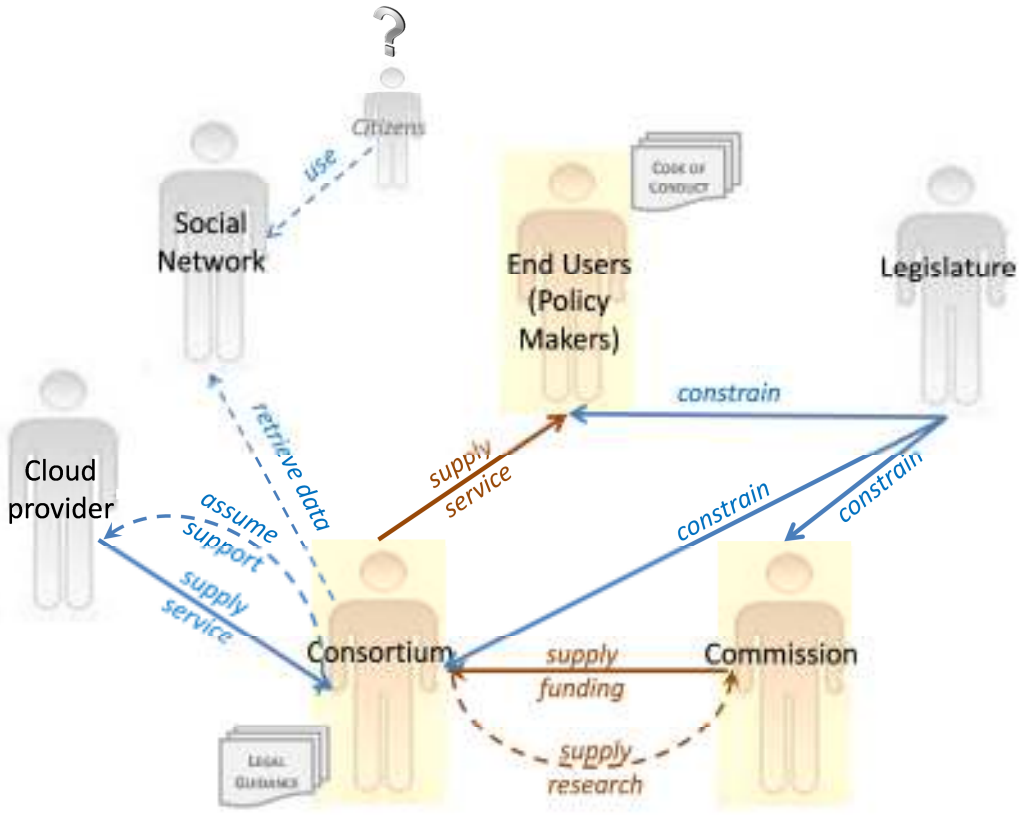

Figure 1: WeGoV stakeholders

The *WeGov* project seeks to capitalise on the popularity of existing social-networking sites to facilitate open dialogue between citizen and Government [12]. The project aims to make available

[3] [14] examines the relationship between expert and novice in policy-making, and the dynamic introduced by online community participation.

the opinions and responses to seeded discussion topics, based on policy plans and decisions, within social networks such as *facebook®*. The data are collated and aggregated by appropriate government agencies to be made available to policy makers to inform and support their efforts. To move the debate forward as well as to demonstrate to users that their opinions are indeed important, policy makers need to provide feedback from their side back to the online community.

Projects such as *WeGov* can quickly run into problems, especially were data protection is concerned. The constraints imposed by such regulation introduce competing and sometimes opposing demands encroaching onto the project as it proceeds. Trade-offs must be made between the level of research *versus* legal compliance *versus* operational evaluation. Basically, the closer a projects evaluation is to operational reality (i.e. using data from real people in a social network) the more representative and exploitable are the results, but at the cost of need to address increased demands for legal compliance. It is helpful to be able to identify and resolve such conflicts as early within the design lifecycle as possible but at a *minimum an understanding of how stakeholders' concerns present potential barriers to adoption is essential throughout the innovation lifecycle.* The basic project scenario outlined in the funding proposal is shown in Figure 1. The *immediate* stakeholders in the project (highlighted in yellow) include the research consortium, the Commission and the end-users. The consortium is funded by the Commission in return for research output; and that output is delivered as a service or toolset to the end users. The end users in this case are *not* individual citizens; instead, they are government representatives charged with analysing and aggregating incoming data as well as providing suitable feedback to maintain and encourage debate. There are, however, other stakeholders. The citizens are involved at different levels and yet are not directly represented within the project. The Government (the "legislature") has significant influence over the project, setting the boundaries and constraints on what constitutes private and sensitive data, as well as how those data can be processed. In addition, the consortium's original proposal included services to be supplied by Cloud providers for large-scale message processing. So these providers are also of relevance to the project and the consortium assumes that they will be able to offer services that can support the type of processing required.

4 A Matter of Perspective

When approaching an analysis of a project, its objectives and concerns there are many possible starting positions, viewpoints and a range of methods that could be adopted. Methods typically originate from a variety of disciplines, and the perspectives they bring have the potential to deliver different insights that can help in understanding how to design Future Internet systems. Our approach in SESERV is to identify a representative set of methods that allows the assessment of social, economic and regulatory dimensions as described in Section 1. We identified that *WeGov* has largely social and regulatory interactions but we also include an economic assessment to understand if a method based on resource contention can have added value.

The questions and issues that the project faces are summarised in Figure 2. The boundaries between regulatory, social and economic concerns are not easy to identify with complete certainty. Providing *incentives*, for instance, may be economic if associated with financial or some other gain, but it is social in terms of social networking sites (SNS's) where individuals are more likely to be incentivised by belonging to a community. But nevertheless, the social, regulatory and economic aspects of the

project are associated with different questions: *how do people engage? what has to be done* to remain within legislative boundaries, and *what is the cost* in terms of architecture and so forth. The methods we use to evaluate the project and seek to find solutions to problems identified, therefore, need to consider these different perspectives.

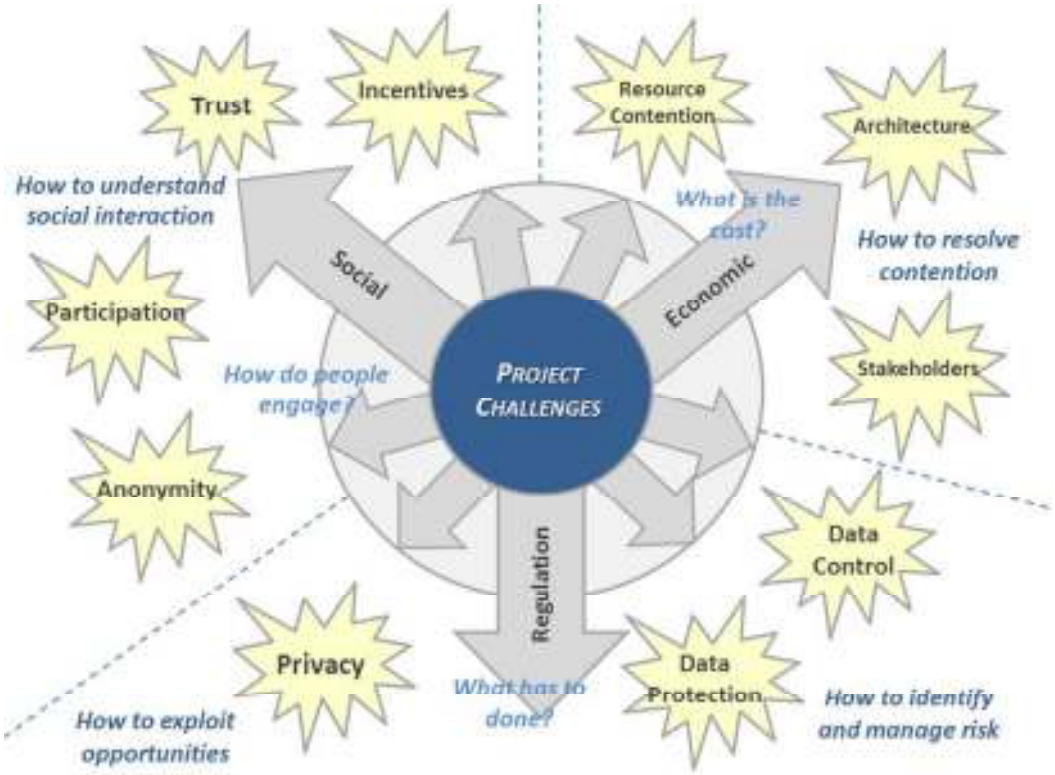

Figure 2: Methods and perspectives

Initially, we use a SWOT analysis as a way to quickly highlight the major project concerns. We then analyse the social issues by considering the properties of collaborative network organisations. Economic issues are examined using Tussle Analysis that has been proposed specifically from the Internet community as a mechanism to help analyse contentions. Finally, we use risk and scenario analysis as a way of identifying risk factors that can affect projects, as well as considering mitigation associated with those factors. In each case, the method is applied to the *WeGov* project and any of the potential issues summarised. Specifically we focus on the objective of data protection compliance and participation for Future Internet research experiments that aim to collect and process personal data from online communities for identification and tracking of political opinion. Each method highlights specific advantages which suggest a different approach to their resolution.

4.1 SWOT: Getting to grips with the issues

To summarise the project, consider it in terms of a SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis. Although traditionally used in connection with business proposals, and lacking some of the rigour of other, more process-driven methodologies, it provides a useful, and easily generated starting point and overview of the characteristics of the *WeGov* project.

This brief survey highlights that the main issues, irrespective of the quadrant, relate to incentives for participation and trust.

- Participation: Do citizens believe that they will be listened to? Is participation more likely within a known social networking context than in a bespoke environment? Can participation be encouraged from representative citizens?

- Trust: Will the data (personal opinion) be adequately protected? Will 3rd parties do their best to support a project that they are not directly involved in? Is participation worth it? (Will citizens be heard?

Strengths	Weaknesses
The project aims to engage with citizens in an environment they already use and understand (social networking sites). As such, users are more likely to continue to be comfortable and to contribute to the discussion, rather than to need time or remain suspicious of a new environment. The discussion fora therefore become an extension of what they know rather than an intrusion.	***Dependency on external suppliers**:* the project is reliant on resources provided by 3rd parties not directly involved in the original proposal. ***Dependency on citizen engagement**:* the project needs citizens to get involved. There may be many different factors which discourage them from so doing. ***Data protection**:* anything to do with data protection tends to cause suspicion on the part of the citizens; as well as much regulation[4]. ***General mistrust of government**:* a manifestation of Big Brother paranoia and the Nanny State interfering and snooping into our everyday lives.
Opportunities	**Threats**
Demonstrate to Government that public engagement is possible in public policy-making without the need to develop new discussion fora or infrastructure. Public demonstration that participation is possible, non-threatening and unobtrusive. Public demonstration that citizen participation *can* make a difference with policy-makers.	***No participation of citizens***: there are many reasons why citizens may not engage. Without them, there are no data to analyse and therefore no input for policy makers. ***Lack of participant agreement to use of data**:* even with their participation, citizens may refuse to allow their opinions to be used for any purpose associated with Government. ***Non-representative participation**:* those who do engage and who are happy with their opinions being passed on to Government may always be vocal and opinionated, and used to voicing their opinions publically. They may not, however, be a truly random sample of citizens. ***Changes in legislation**:* given the sensitivity surrounding data protection, new regulation could mean that different, more stringent measures are required, or the opposite: that much effort was expended to protect data which is not subsequently necessary.

Table 1: SWOT analysis for ICT *WeGov*

The issues which the SWOT analysis seems to highlight are neither financial (economic) contention[5] nor technical (infrastructure) in nature[6]. The project in general revolves around novel or extended *use* or applications rather than how such use might be supported.

[4] *Data protection* and *privacy* tend to provoke strong, and often, negative public reaction. This can be the result of a loss of data (well-publicised cases of computer theft or other governmental failure to protect data) or stirring up opinion around *Big Brother* and the loss of civil liberties.

[5] The issue around dependency on 3rd parties (for data processing) could, it might be argued, be reduced or even removed with sufficient economic incentive. But this is a *solution* to a potential issue; not the issue itself.

[6] It could be argued that issues of participation and trust could be associated with both social as well as economic motives. For instance, participation for someone in full employment and a busy private life may seem worthless (what is called "opportunity cost" in economics); for someone who is not employed or retired, it may be quite the opposite.

4.2 Collaborative network organisations: Design from the users' perspective

In this section, we use a socially-based approach, or rather body of work, as a way to examine participation models in *WeGov*. In a number of related studies, Dutton and co-workers have explored issues related to user participation in online services [4, 5 and 6]. Starting from the bold assertion that:

> "All technologies are inherently social, in that they are designed, produced, used and governed by people"[7]

They regard:

> "Understanding relevant social and institutional dimensions [...] a key priority in addressing the way these technologies affect trust, crime and related issues" [6:28]

In the context of individual participation in online communities, there are a number of fundamental assertions, which ostensibly emphasises the social dimensions of projects (see Figure 1 above) rather more than the economic or regulatory. Yet, what Dutton and colleagues present is convincing evidence of a different set of criteria to regulation ("legislation" in Figure 1), motivation through financial negotiation ("economics") or through collaborative engagement ("society"). Dutton and Shepherd, for instance, suggest that *cybertrust* should be viewed in more generic terms in the same way as individuals do: an everyday "confident expectation" that what they wish to be protected will be. Further, there is clear support for a view that frequent, or more familiar users are likely to have more realistic expectations around privacy than novice users despite more negative experiences such as spamming that their greater usage generates [6:25 and *passim*]. People adapt and learn to set their own boundaries [*op.cit*.]. This is a very significant finding indeed. The implication is that irrespective of any regulatory prescription, whatever the technical infrastructure provides in terms of privacy and data protection will be used by individuals as *they* wish. Privacy is to do with people's experience and expectations, therefore, and not what government lays down[8].

In exploring personal interaction with the Internet and online communities, Dutton defines a simple typology of individual engagement with networked facilities or communities:

1.0 ***Sharing*****:** relating to networks of individuals who simply share information and data; participants post content for all to see and refer to;

2.0 ***Contributing*****:** describing networks or communities where individuals or user groups assess aggregate and comment on content, so that all can benefit from such evaluation; and

3.0 *Co-**creating*** **(or *Collaborating*):** in which individuals collaborate to create, disseminate and monitor content[10].

[7] Dutton, W.H. (1999) *Society on the Line: Information Politics in the Digital Age,* OUP, Oxford and New York; cited in [6]

[8] The point is this: experienced users set their own expectations as determined by their continued use of a service, often independently of whatever the technology provides. *facebook(R)*® may offer better security settings, for instance, but that alone will not necessarily affect the trust level of experienced users. One example that Dutton and Shepherd quote is that even spam eMails will not deter experienced users from continued use of online services.

Alongside this typology, he explores issues such as the need and role of management (of individuals as well as content, and the moderation of fora), the social underpinnings of participation, and the technical requirements associated with the platforms supporting the network. Although discussed and presented primarily in the context of more formalised communities (including social networking and collaborative work) [4], establishing what relevance this typology as well as observations around cybertrust and user experience have to *WeGov* will help identify what a social analysis might bring to this type of project.

As outlined above, *WeGov* directly engages members of the general public in political discussion using existing technologies (SNS) for the purpose of aggregating content. As such, the perception of those users of the Internet and how they engage in online communities is of particular importance, but in addition, how that community of citizens is supported technically and how the opinion gathering exercises are managed are key factors in the design and development of the deliverables. It is vital that transparency is offered and maintained in this context: citizens need to be kept informed of what is happening to the information (the opinions in this situation) they offer. Let us focus primarily on aspects of participation, which was identified as a particular concern in the introductory SWOT analysis.

Consider first the typology of citizen participation, summarised in Table 2 with respect to the underlying architecture as well as aspects of the processes associated with the interactions[9] within the different types of collaborative network organisation (CNO).

Mechanism	**1.0[10] Sharing**	**2.0 Contributing**	**3.0 Co-creating**
Architecture	One-to-Many[11]	Many-to-Many	Many-to-One
Openness	Open	Networked	Managed
Control	Low	Moderate[12] (reputation)	High
Modularization	Low	Moderate[12] (simple tasks)	High

Table 2: Collaborative Network Organisations (CNO) typology (*from [4]*)

The underlying *architecture* for each CNO type needs to support interactions from those based on one individual communicating with many, to those where many individuals work together to produce a single output (code or documents generated by a whole team using collaborative development tools, for instance). The architecture "mechanism" is fairly obvious and straight-forward. Any specific technical issues arise from the interaction types. For instance, within 3.0 Co-creation, collaborative tools need to support functional ownership and version control, whereas in 1.0 Sharing, the only requirement is for some level of naming convention and control.

The other "mechanisms" and terms require some explanation. *Openness* and *Control* refer to the degree to which individuals and the content they produce or view needs to be managed. For

[9] In the original discussion, interactions are between direct participants within the CNO. For *WeGov* this would include both the citizens offering their opinions and the policy makers providing feedback.
[10] 1.0 – sharing hypertext documents, data and other digital objects; 2.0 – deploying social networking tools to support collaboration and generate user-content; and 3.0 – applying collaborative software to support cooperative co-creation. [4:215]
[11] The "one" and "many" here refer to participants engaged in sharing or collaborating.
[12] The ambiguity in the use of *moderate* is in the original and probably not intentional.

instance, within a 2.0 Contributing CNO, users of a community which provides technical know-how or support such as the SAP Community Network (SCN) tend to be self-regulating in terms of contributions and especially who is an expert and who is not (*Control* is via moderation). Similarly, in a 3.0 Co-creating environment, the *Openness* or access to the network as well as content is managed so that only those with a legitimate reason to be participating can. The final line of the table, *Modularization*, refers to the extent to which work or interactions need to be split into smaller, more manageable chunks: in a 1.0 Sharing environment, all tasks tend to be simple and self-contained: a single user will format, write and check an entire document, for instance. In a 3.0 Co-creating CNO, by contrast, individual sections of the document, as well as proof-reading, overall look-and-feel and so forth would be distributed tasks broken down and assigned to individual contributors.

In related presentations of this CNO table (see [5] and Table 3), Dutton extends the considerations associated with a given type to include the concepts of content ownership (Intellectual Property Rights – IPR) and evaluation (Performance: how do we know whether the CNO is successful or not?). For instance, in a 1.0 Sharing organisation, the Intellectual capital needs no protection *per se*: it is acknowledged and accepted as public and shared, by definition. In addition, if we wanted to assess how *good* or relevant that shared information might be, then for a 3.0 Collaborating (previously Co-creating) environment, the number of appropriate individuals adding to the overall output – that is not just who is contributing, but are they the right contributor – is the main measure.

	1.0 Sharing	**2.0 Contributing**	**3.0 Collaborating**
Architecture	One to many	Many to many	Many to one
Openness and Control	Open, Low Control	Managing access	Tiering, management control structures
IPR	Information shared	Platform	Co-created product
Performance	Viewers	Quantity of Contributors	Engaging targeted experts, producers

Table 3: Issues of Control, Ownership and Evaluation with CNOs (*from [5]*)

So what is the importance of this typology for *WeGov*? The implication of these tables is that once we have identified where *WeGov* sits in the typology, then architectural, management (openness and control), ownership and community evaluation (performance) types will all have been determined and can be appropriately addressed. Say, for instance, *WeGov* were seen as a 2.0 Contributing project, then we could evaluate the architecture on the grounds that it needs to enable many individuals to contribute to many items; access would need to be managed (not everyone can join; and not everyone can contribute on everything); the content is "owned" by the platform itself, not by the individual contributors and not as part of an overall, aggregated output; and the number of people getting involved would be a measure of its success.

This presents an interesting problem. The implication in related work[13] (see [4 and 5]) is that organisations will tend to fit into one type or another, and this does inform the way they work and

[13] Dutton analyses a number of different types of CNO, ranging from the likes of *Bugzilla* to *A Swarm of Angels*.

should be set up. For *WeGov*, then it actually depends on the perspective taken. From a Government-as-beneficiary viewpoint, then this looks very much like a 3.0 Collaborating project. The hope is that many individuals will engage to provide their political opinions; there needs to be some management of the input to ensure that contributors are not exclusively activists with particular and extreme views; in essence the consensus that results is a "co-created product"; and its success or otherwise will be judged on the quality of the contributions – again, they would prefer informed opinion rather than bias and prejudice. This has various implications. For example, if the consensus is to be viewed as a "co-created product", then it would be important to secure rights to the original individual opinions, or to request consent from those expressing those opinions. Similarly, it places an emphasis on some kind of aggregator – the result of many-to-one contributions – to marshal inputs into a suitable consensus, whilst maintaining the integrity of individual views. This would make *WeGov* a data processor, in data protection parlance, not a controller which in itself has important consequences for the handling and storage of the opinions collected. As such, *WeGov* enables the collection of data (public opinion), will effect some analysis (such as aggregation) and then passes those data on to the policy makers, who might store the data as well as review and develop ideas based on the opinions expressed. The policy makers, as operators of the *WeGov* services, act therefore as data controllers.

An alternative view though would be to consider the citizens' viewpoint. For a typical, open debate (i.e. posting messages on a social networking site, or SNS), then the 1.0 Sharing type seems much more appropriate. An individual will express a view and this will be made available to many: the architecture should be one-to-many, therefore – a message board or chatroom or similar. There is little control; from the outset, the opinions offered are shared and public; their value derives from how many other people view and comment on them[14]. Data protection is of little relevance here, beyond the need perhaps to dissociate particular individuals from particular opinions (protecting individual identity[15] and not the view expressed) because by definition the SNS as a 1.0 Sharing type provides a forum for individuals to broadcast content to anyone and everyone else. Of course, the architecture and behavioural paradigm fit this type perfectly: Social Networking Sites. They are set up for individuals to express views and broadcast them to all (where "all" is optionally anyone who should access the site, or the trusted circle of cyber friends identified by the individual). There is little control, and moderation if any tends to be on an *ad hoc*, self-regulatory basis. The "performance" of any individual is very much judged on the basis of how many posts are received in relation to what they started, assuming there are no spammers or other such inappropriate behaviours .

Since the type of CNO changes depending on the perspective (Government-as-beneficiary *versus* Citizens), it is tempting to conclude that CNOs may not be the right way to approach the project at all. Instead, something which categorises the project into one type or another seems preferable. But this, in fact, is not the case. The various typologies highlight the different expectations of those involved as the real actors: the citizens providing the inputs, and the Government (or policy makers) as beneficiaries of those inputs. The challenge for the *WeGov* project is not so much blanket conformance with all the regulation associated with data protection, but simply to match the requirements of a 3.0 Collaborating CNO with those of a 1.0 Sharing one. Effectively *WeGov* needs to

[14] Comments could be semantically parsed to categorise them into broad *agree/disagree* measures.

[15] Here, SNS's provide a useful precedent derived from traditional broadcasting: individuals may "anonymise" themselves either with completely random pseudonyms (*Trekky, Golum* etc) or more informative (*35yoMumof2*)

interconnect two systems supporting different CNOs considering approaches to architecture, openness/control, IPR and performance. As such, data protection is reduced solely to what is actually required to maximise collaborative interchange. Figure 3 summarises this for *WeGov*. Citizens trust the online community as a 1.0 Sharing environment and will therefore participate fully to offer opinions and views. The "end users" in the sense of government representatives, using the *WeGov* toolset in aggregating the data available on the SNS, operate as a 3.0 Co-creating network providing opinion to the policy-makers. There are two CNO's in operation here, then.

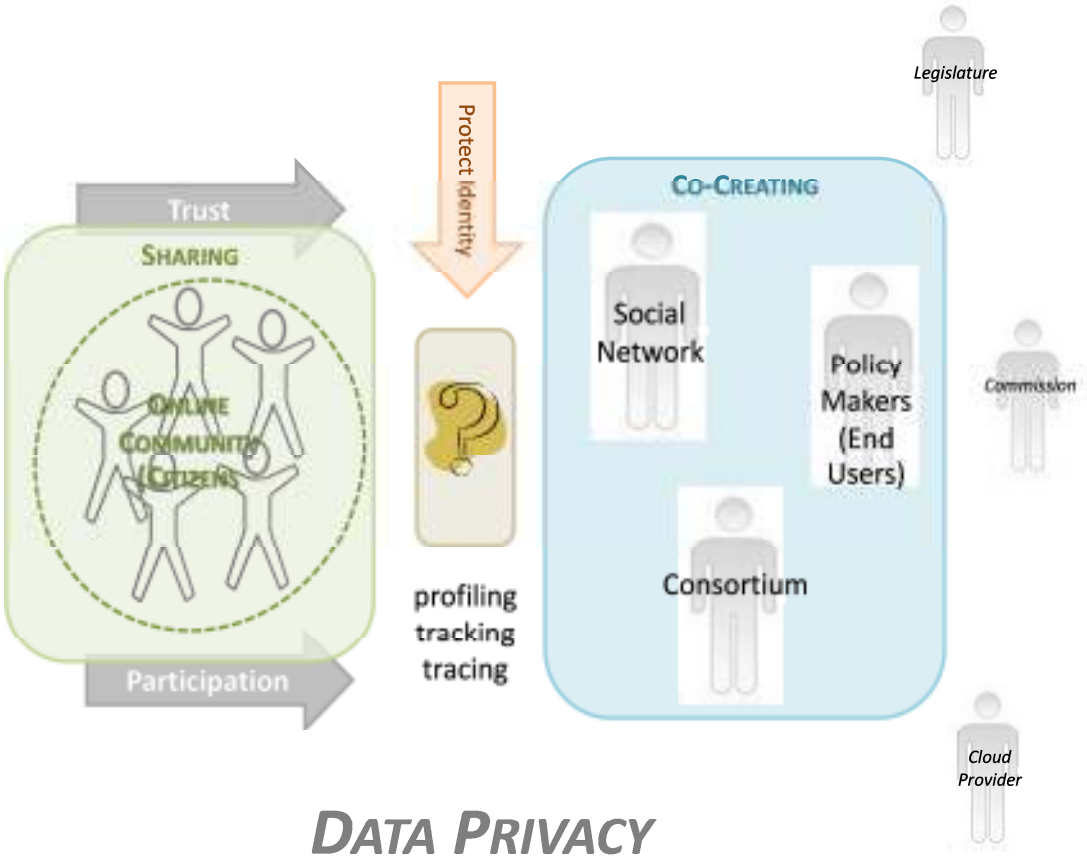

Figure 3: A different *WeGov*-centric view on data privacy

What everyone wants from the online community using the SNS is their participation, which in turn requires trust. For *WeGov* there are at least two different sets of relationships that are relevant: on the one hand, the online community itself would hopefully continue to run as normal; it is a 1.0 Sharing CNO. On the other, the Consortium, the SNS (indirectly) and the End users collaborate to generate the required output, namely public opinion. In this, they function as a 3.0 Co-creating or Collaborating CNO. Privacy as maintained through data protection is now not so much a question of implementing all appropriate security measures to ensure the protection and integrity of the data. Instead, it is a guarantee that individual identities will be shielded: there should be nothing to connect the opinion with the person or persons who expressed it. As stated above, *WeGov* as a project needs to be able to connect and map the two CNOs effectively to succeed, and in so doing should be guided by the trust requirements of the online communities to ensure and maintain their participation.

The technical issues can be summarised in terms of what is required to allow maximum input[16]. There are few economic issues in the financial sense, unless there is to be some licensing of data or modest payment to users; or in the sense of increased burden or contention for resource, given that there is no particular requirement to increase activity beyond current levels. Socially, the focus is on self-regulation (the number and types of comments and response-chains) and the potential - when married with the 3.0 Collaborating type required to process the opinions for policy-makers – removal of specifics which identify any individual[17]. The regulatory or legislative considerations are far more focused and confined than might previously have been thought.

	1.0 Sharing The Citizens' Input	**3.0 Collaborating Government use of that input**
Technical	Requires a one-to-many platform, allowing open, relaxed interaction and the free and open sharing of ideas and comments in response to those ideas.	Requires many-to-one aggregation of inputs, with some filtering and "control" associated with who can and cannot participate. The output is a co-created consensus of opinions.
Social	Participants are used to offering views and comments freely and without restraint in an SNS environment. There are inherent cybertrust boundaries that can be exploited in SNS's, which have been developed by users to manage and regulate their own and other inputs.	The issue is one of respect for individual views and the protection of those expressing those views (their identity).
Management	Very little required. Most inputs will be self-regulated.	Some control of who can participate. Perhaps some different levels of participant or participant type could be tried.

Table 4: CNOs and *WeGov*

In summary, the CNO type depends on the viewpoint. Input from individual users and subscribers to SNS's is very much a 1.0 Sharing environment, where opinion is freely offered within the context of known social interactions. How those views are processed for the policy makers is more a 3.0 Collaborating organisation: data are aggregated and processed to extract common themes and responses. Table 4 brings this together. In reviewing the typologies implied by the general public on the one hand and the government/policy makers on the other informs the decisions which really are important for the *WeGov* project.

Support Outcome	**Comments**
Constructing issues and research challenges	The Social Analysis (an abstraction of Dutton's CNO concept) approach has highlighted that *WeGov* is really about marrying expectations and requirements from two different well-established types. This could lead on to the identification and pursuit of a range of different challenges related to the mapping of expectations and practices from one area to the other. Identifying and addressing any issues which arise from the coexistence and potential interdependence of these two types is no longer really about data protection legislation.

[16] Note that there is no discussion here of filtering input on qualitative lines; the value of any opinions or comments will tend to be self-regulating in that participants will decide for themselves what constitutes good and poor inputs.

[17] Anonymisation – removing anything which might associated data with its source – is not a trivial operation, and may not be completely successful. For one thing, to anonymise data, the original personal details and data need to be processed which means that strict data protection is still required at some stage in the proceedings.

Support Outcome	Comments
Facilitation of communication and debate	Typing the contexts in which the main groups – the public at one end and the Government at the other – helps to identify and describe what is and is not important to each group. Should problems or concerns arise, then this provides a context in which questions can be raised and worked on jointly.
Assessment of technology advances	Not at this stage: the technologies at either end are well understood (and currently available). The main issue is mapping the two environments. The success of that mapping could indeed provide some way to assess technology innovation.
Improving engineering design through insights from other domains	By definition, viewing the "trust" of participants in a CNO from a social rather than technology point of view has led to a different assessment of the design issues.
Designing legally compliant Future Internet experiments	The approach has highlighted what *really* matters to users in terms of trust and data protection. This helps to refocus regulatory concerns – users of the *WeGov* services operate at most as a data processor rather than controller; identity protection is more important to the user, but can be handed off to the user[15] rather than pose technical challenges.
Improving project design and decision making	Typing the essentials from the viewpoint of users and beneficiaries has provided a different, and hopefully more informative, perspective which would benefit issue identification and resolution.

Table 5: How useful is *Social Analysis?*

4.3 Tussles: Design the playing field and not the outcome

Prompted by an "important reality that surrounds the Internet", tussles first began to be formalised and discussed in 2002 [3[18]]: as the result of a DARPA-funded research project:

> "different stakeholders that are part of the Internet milieu have interests that may be adverse to each other, and these parties each vie to favour their particular interests" [*op.cit.* Abstract]

The paper discusses many aspects of contention within network architecture and operation. But the basic tenets are these:

- Engineers design for predictable outcomes;
- The Internet grew up on that basis – ie., an engineering construct for high and reliable performance;
- The Internet has now changed into a more social animal, as a result of the users who have claimed it for their own; and so
- The engineers designing for it now need to design with contention in mind.

Much of the limited derivative work[19] has been focussed on network-centric issues of protocol enhancement and business models affecting ISPs and the ASPs that depend on them, though some have picked up on the original "social animal" allusions in the original paper. On the network-centric, non-user side, Sollins [11], for instance, suggests that a tussle approach can help identify and resolve

[18] The 2005 IEEE version of the SIGCOMM'02 paper has only minor updates.
[19] *Google* claims that there have been 381 citations of the 2002 version.

issues relating to network management, though this is an assertion which is not fully developed or explained. Similarly, Koponen et al [8] cite the tussle approach as helpful, but then do not specifically apply it to their main focus: the problem of DNS servers. In contrast to these purely technology-based discussions, Bestavros [**1**] spends about equal time on technical issues such as domain name servers, routing and net architecture, as well as real usage, in terms of individual privacy, copyright infringement and Big Brother type activity tracing. His overriding message though is that it is time for coders to embrace the new reality of the Internet as a social instrument and to design for variation in outcome as opposed to a single predictable result. Brown [2] by contrast explores the relationship between regulation – what the law makers attempt to define and protect – and what can and should be done to protect the reality of civil liberties such as freedom of speech and privacy. For Brown, "tussles" are not only or even principally about the economics of Internet operation; he is much more interested in how the Internet can respond to its implicit responsibilities to those who use it in good faith. Clark too introduces a social dimension for trust in network usage: someone who receives a call may choose not to accept it. Tussles seem to be a promising suggestion, therefore, to begin to come to grips with issues of contention for the architecture and economic management of networks, but as yet there is little evidence that they offer any more than a taxonomy for contention definition. What is more significant, though, if the Internet really has become more a social instrument than just a technically intriguing challenge, we might begin to wonder whether a tussle methodology focuses on the trees rather than the proverbial wood.

In trying to explore the usefulness of the tussle approach, Kalogiros et al [7] attempt to codify the methodology and define the types of contentions ("tussle patterns") that may be expected. They suggest the following process to analyse any given tussle:

1. Identify stakeholders;
2. Identify tussles among stakeholders and their relationship; and then
3. For each tussle:
    a. Identify how control is distributed between stakeholders;
    b. Assess impact where control is not in balance;
    c. Identify whether a subset of disadvantaged stakeholders could gain more control by whatever means.

Further, they identify a number of tussle categories or patterns:

Tussle Pattern	Description	Possible Resolution	Example
Contention	Two or more parties (consumers, or consumers and suppliers) wish to exploit the same resource.	Through restoration of economic equilibrium or external regulation.	Use of cloud resources, resulting in bandwidth contention (even malicious *bandwich*).
Repurposing	A resource is used for a purpose not originally envisaged (or paid for).	Restrict access to / capabilities of the resource(s).	Sharing copyrighted materials; selling on personal information.

Responsibility	Resources are used for purposes not acceptable to original provider.	Difficult to resolve because some agent has to defend rights of non-associated 3rd party.	Distributing content protected by rights.
Control	Multiple resources (or actions) determine the outcome.	Restrict usage of other resources to force dependence on individual supplier.	An ISP trying to restrict consumer to their own VoIP offering, rather than accessing any other offerings.

Table 6: Tussle patterns from [7]

The tussle patterns may be of use in trying to categorise and thereby characterise general contention types, that may be of relevance to other projects as well. There is a concern, though: the description of the issues here is very much on the basis of the economics of resource exploitation. We need to restate the description with more of a focus on the services and activities run on those resources, rather than the resources themselves. The intention here is to generalise the patterns to be more applicable to social interactions enabled by the Future Internet, and not just the economics of developing or running such an infrastructure. The table below is a first attempt to broaden the patterns out to include applications or interactions, whilst maintaining the same classificatory intentions.

Tussle Pattern	Description	Resolution	Example
Contention	Two or more parties have conflicting interests around the same issue.	Through negotiation, consensus, compromise, or withdrawal.	Agreeing the price of a contract; negotiating terms; and so forth.
Repurposing	A party uses something for a purpose not originally intended.	Litigation or economic sanction.	Asking people to respond to a survey, but using responses for targeted marketing.
Responsibility	A party knows something is being done, which is inappropriate, but is not motivated to do anything about it.	Whistle blowing.	An ISP is aware that a Government is monitoring web use for surveillance purposes.
Control	Multiple claims on the same data/resource.	Enforcement of terms and conditions or other usage constraints.	Collecting one set of data for multiple purposes.

Table 7: Tussle patterns - a more generic approach?

This discussion provides a useful framework against which to analyse any given contention. In fact, they apply their methodology to a number of existing projects, if nothing else to establish the tussle pattern associated with a given issue in a given project[20]. We now return to *WeGov* and provide two example tussles from the project.

Government *vs* Consortium, End-Users, Commission: *Control Tussle Pattern*[21]

[20] They reviewed *Trilogy, ETICS, SmoothIT, MOBITHIN* and *SENDORA*.

[21] In this section, we consider *WeGov* solely from the perspective of what the project is doing internally, and not with the broader issue of how the results and data of the project may be used outside the project.

The Government is the legislature that generates any and all regulation. It is up to the Consortium, the end-users and the Commission to respect and comply with it. For the Consortium, the legislation may limit their ability to explore all of the potential from the data made available to them. Further, it imposes obvious requirements on what they produce in terms of tools and services, all of which must conform to the same legislation. The end-users are bound, of course, by the working practices and requirements of their employers (the Government), but more importantly cannot be seen to deviate from the law: even when operating within the law, surveillance for instance could be very damaging to their reputation. They are ultimately dependent on the Consortium to provide them with some level of protection against inappropriate use of the data (see above), even if such protection may have to be in the form of advice and guidance. Finally, the Commission has to ensure that no project contravenes any legislation, as well as complying itself. There is a burden of enforcement on them to some extent, but more importantly, they may well be more open to reasonable compromise in the case of *WeGov* since it is in their best interests as well as of the Consortium to work together to ensure complete compliance to data protection laws, whilst extracting the maximum benefit from the data on offer.

We describe this as a "control" pattern, since Government regulation will ultimately bound whatever use is made of the data in *WeGov*, even though different parties may wish to use the data in different ways.

- *Control:* anything involving regulation will tend to be weighted in favour of one of the stakeholders: the balance for this tussle is firmly tipped in favour of the legislature. This fails, however, to see the Government in a different stakeholder guise: they *want* to get the data from the general public on policy proposals and so forth, cynically to give the impression of encouraging participation, but equally perhaps in a genuine attempt to ensure that everyone is heard. In this case, *control* is more evenly distributed. It is the general public who can exert the greatest influence, mainly through non-participation. With the Government as this kind of participant, then the tussle is balanced.

- *Impact:* failure to comply with legislation generally involves punitive sanctions - financial (fines) as the result of legal proceedings. In the case of the unbalanced, regulatory tussle described first above, the Government has the power to disable any of the other stakeholders. This could have far-reaching consequences not confined to the present project.

- *Disadvantaged stakeholder moves:* there is little scope for the Commission, the Consortium or the end-users to try to redress the balance. However, there is always the potential to push back and try to effect a change in legislation: if regulation prevents any usable data becoming available, there is certainly an incentive for the Government to show some flexibility. This is viable only when the Government has both of the two different stakeholder types mentioned previously: although the ultimate regulatory authority, they are also a significant beneficiary if the project succeeds.

This tussle illustrates the phenomenon that stakeholders may have different interests, depending on the view taken of the specific tussle. On the one hand, the Government hold all the cards. They are responsible for the legislation, and expect and require compliance. On the other, they are a

beneficiary of the work to be performed and therefore have some motivation to see regulation changed to allow them to get the most out of what is on offer. Designing for this tussle would be difficult, therefore, since the same player becomes involved at different times in the same tussle with different vested interests. It may be that designing network infrastructure is a rather simpler task than handling contract negotiation. We conclude that contention between government and Consortium, End-users and commission, does not fit easily within the tussle paradigm.

Consortium vs Cloud suppliers: *Responsibility Tussle Pattern*

The Consortium had initially proposed using Cloud facilities to process incoming data from users (the citizens). Political opinion falls into the category of personal data requiring protection and specific security measures when processing. Cloud providers do not, however, typically meet these security criteria. The Consortium may not, therefore, recommend those facilities to be used to process personal data.

This tussle relates directly to economic considerations. Cloud providers do not currently provide the security features required when handling personal data. To implement them would require investment, increased operating costs and potentially constraints of operational practices (i.e. restrictions on policies for virtualisation). Without a sufficient business case, there is no incentive for the Cloud suppliers to make such a change to their facilities. Government regulation is not a significant enough argument: they support and make a business out of other resource-intensive activities which do not require such measures. It is theoretically possible that the Consortium might fund some of the work needed, though this is highly unlikely and would be difficult to justify. Why would public funding be used to bring a supplier into regulatory compliance?

As such, there is an impasse. To exploit Cloud facilities as the Consortium describe in their original proposal to the Commission may result in significant increases in operating costs due to the extra burden of ensuring adequate data protection compliance. Regulation provides safeguards; it is not typically used to impose business strategy. Since this is about who should take ownership for what, this is a “responsibility” tussle.

- *Control*: the tussle is weighted in favour of the Cloud suppliers, in that there is little the Consortium can do other than offer to fund or financially support the investment needed.

- *Impact*: the Consortium finds it difficult to fulfil the statement of work within the secured funding from the Commission. To avoid project cancellation or other sanctions, the Consortium may need to negotiate a modification to the statement of work, for example, hosting cloud services within the consortium or outsourcing work to a data protection compliant hosting provider.

- *Disadvantaged stakeholder moves*: there is little the Consortium can do as far as the Cloud suppliers are concerned, since financial support is not a feasible option. Were they to attempt to put forward a business case to make the necessary investment by the Cloud suppliers attractive, they would still be delayed in what they could deliver and when.

This additional aspect of the issues surrounding data protection for the *WeGov* project most closely approximates the classic tussles described elsewhere ([**3**, **7**, **8** and **11**]). It is very closely linked to the

economics of providing network capabilities to support a given function or set of functions. "Designing for the playing field" of data protection [**1**] would have required Cloud providers to support the rapid integration of suitable data processing extensions, such as encryption and access control as well as the management of monitoring or other mid-path stations within the network itself that might divert or interrogate the data inappropriately.

For both examples above – the *Control* tussle between Government on the one hand and the Consortium, End-Users and the Commission on the other; and the *Responsibility* tussle between the Consortium and Cloud suppliers – it would be possible to repeat the analysis specifically around the issue of research drivers, regulatory compliance and the reality of participation in SNS. This may lead to the identification of yet more options for the disadvantaged stakeholders to attempt to regain some level of balance through the creative use of technology (solutions based on encryption, for instance) as well as architectural implementation (including distributed processing to make it more difficult for a third party to access all but a small proportion of the overall dataset). For now, though we will confine ourselves to the two illustrations here which suggest two extremes: in the first case, a less-than satisfactory set of conclusions in respect of stakeholders, and in the second, a rather more "classic" tussle problem.

Supporting Outcome	Comments
Constructing issues and research challenges	Focusing on stakeholders and the relationships between them helps to begin to look at potential problems and issues. At that stage, there is much scope for investigative work and research. Specifically for *WeGov*, tussle analysis has revealed more about relationships and dialogues to be had between different direct and indirect stakeholders rather than actual research or development topics.
Facilitation of communication and debate	There is some indication that tussles have helped establish what the issues are and who needs to be approached.
Assessment of technology advances	New security mechanisms.
Improving engineering design through insights from other domains	N/A
Designing legally compliant Future Internet experiments	The tussles have indicated what should be considered in respect of legal compliance. It is difficult, however, to establish whether this was not obvious in advance.
Improving project design and decision making	To some degree. The tussles outlined have tended to show what needs to be taken into consideration and who needs to be approached for discussion and negotiation.

Table 8: How useful are Tussles?

4.4 Risk management: Design for outcome considering uncertainty

The most obvious approach to achieve legal compliance is to adopt a risk management approach. With its roots in safety and security disciplines, risk management has been applied to many different areas and scenarios, from biohazards [9] to standard business planning [13], and has even been standardised [10]. ISO/IEC 27001 stipulates that a risk analysis method should be used, but the method is not a part of the standard, and no specific method is proposed, apart from integrating the PDCA (Plan, Do, Check, Act) recursive process of the model as defined for the creation of the ISMS (Information Security Management System). ISO 27005 [15] was recently published (04 June 2008)

to provide guidelines for information security risk management and to support the general concepts specified in ISO/IEC 27001. However, implementers are left to devise their own methods consistent with these guidelines. EBIOS [16], MEHARI [17] and OCTAVE [18] are all examples of risk management methods.

In general, risk management is an on-going process designed to assess the likelihood of an adverse event occurring, implementing measures to reduce the risk that such an event will occur and ensure the organisation can respond in such a way as to minimise the consequences of the event:

> "Risk may be defined [...] as the probability of occurrence of an adverse outcome and the severity of the consequences if the outcome does occur" [It] must be directed towards assisting those responsible for making decisions to do so in a way which is consistent with scientific principles, legal requirements and public values" [9].

Unlike tussles, where the by-word is design for variable outcomes, risk analysis focuses on a specific objective. In the *WeGov* project this is data protection compliance for Future Internet research experiments that aim to collect and process personal data from online communities for identification and tracking of political opinion. To address this objective the project adopted a risk management approach building on deep technical and legal expertise [20].

As preparation for risk management a legal analysis was performed by the *WeGov* project use cases in relation to the principal EC Directive regulating the processing of personal data: Directive 95/46/EC9. The main challenge is to understand the implications of information processing that crosses different legislative (US to Europe) and administrative (*facebook®* to Policy Maker) domains. The legal analysis starts by identifying the processes of each use case including monitoring on SNS, consent and fair processing information notice on SNS, extraction, and topic injection. For each process an examination is made on how privacy and use policies of specific SNS (e.g. *facebook®* and Twitter®) relate to legislative roles and obligations. In some cases recommendations are made for compliance such as limiting the scope of the *WeGov* toolset's search to only those comments of users that have joined an official *facebook®* Page or a group set up by the Policy Maker, thereby obtaining explicit consent (via opt in) from the site user. The project then uses the OCTAVE Allegro risk management method to identify risks and security requirements that need to be implemented by the project for compliance. The outcome of the analysis is a risk measurement criterion in relation to impact areas for Policy Makers, profiles of critical information assets, threats to those assets and security requirements that should be implemented to mitigate the threats.

Some risk management approaches [10] encourage the consideration of opportunities as well as threats in all stages after risk identification. This is not included by OCTAVE and therefore was not considered by *WeGov*. Without going into specific detail on all of the risks identified, it is clear just how pervasive the data protection issue is for the project. At one level it affects *Research and development*, *Intellectual capital*, *Reputation* and *Data loss*, the main concern associated with data protection, but also *Citizen demotivation* and in consequence *Public opinion*; *Consortium collaboration* and *deliverable schedule*: internal issues which could be affected by any actions taken in response to data protection concerns within Clouds. For each of these areas, it would be possible to consider the threats and opportunities that result.

The opportunities and threats shown in Table 9 provide yet another perspective on the issues facing the *WeGov* project. Looking at threats – and again this is not a quantitative analysis – these help to prioritise the issues and concerns. Without such prioritisation, time and effort may be wasted on matters of little overall importance and beyond the direct control of the consortium. (Note, however, that there is no explicit division here into internal and external risks.) On the other hand, the opportunities shift the focus from the problem into the solution. This encourages problems to be viewed in a more positive light and as part and parcel of any project.

Risk	Opportunity	Threat
Research and development	Develop new techniques to analyse personal data which protects the rights of the individual providing those data.	Work could be sanctioned (halted; no funding) without tangible and innovative returns.
Intellectual capital	Explore what can and cannot be done with anonymised data. This may result in a pragmatic decision that this is impractical, which in itself would be of value beyond the project to others in similar situations.	Without a creative approach to the issues, nothing will be generated.
Reputation	Demonstrate that valuable work can be achieved even under regulatory constraint. Explore and question regulation.	Dependent on compliance, but also project execution. Reputation loss is a significant problem for government and government representatives alike.
Data loss and leaks	Introduce appropriate measures and procedures to protect data. Embed expiration handling.	Public outrage. Lack of participation. Project funding risk or other sanction.
Citizen demotivation	Engage directly and frequently with public to encourage involvement and see the benefits of the work. Enable feedback from policy makers to maintain participation and debate.	No data to analyse.
Public opinion		Constraint on future funding.
Consortium collaboration	Discuss alternatives internally and with project office involvement. Refocus work.	Failure to deliver project content or on time.
Deliverable schedule		
Regulation	Explore potential for regulatory change. Exploit Government as beneficiary of project to present a case for change.	Constrains any innovative work.

Table 9: Generalised opportunities and threats resulting from risk management

Throughout the process there is an emphasis on communication: let *all* stakeholders know what is going on. Although the methods do not specifically attempt to provide guidance on how to identify those stakeholders, it is an essential step to keep decision-makers informed about the findings and recommendations of the experts engaged in the risk assessment. In applying risk analysis to *WeGov*, we are not confined to economic or regulatory concerns amongst those with a vested interest (the stakeholders or decision-makers) in the work. Instead, we can review and prioritise what the real concerns are and are encouraged to look for solutions before we even begin, and whether or not

those risks should become a reality. What is more, in exploring both the threats (the negative outcomes) and the opportunities posed by the risks we have identified, we are able to present a clearer and more balanced picture and action plan to all stakeholders and the public. This communication is a significant and essential part of the process. Where trust and participation are concerned, communication is also a must. So risk analysis looks for solutions to problems, and not just their characteristics, emphasises open communication with all concerned, and is not constrained to any particular domain. It therefore has a broader and more generic applicability than tussle analysis.

Support Outcome	Comments
Constructing issues and research challenges	Around specific objectives, risk analysis can highlight the potential solutions (mitigation strategies) to address problems. Such solutions represent key focus areas for research and targeted development. There is a problem, though, that the objective of the risk analysis is generally confined to a specific issue. As such, unless the technique is tried many times on different areas of risk, items will potentially be missed.
Facilitation of communication and debate	Risk analysis includes communication and feedback between all parties. Since the process involves some thought and discussion around potential solutions or at least mitigation (areas which can direct effort and research), then it provides a complete overview to help articulate problem *and* possible solution.
Assessment of technology advances	Technology improvements or enhancements can be identified and evaluated readily: these will occur as implementations of the potential solutions identified previously. However, once again, unless *all* aspects of the project are reviewed, some technology advancement drivers may be lost and thereby their potential solution.
Improving engineering design through insights from other domains	There is no specific involvement of external expertise. However, discussion around potential solutions can help identify where expertise is required.
Designing legally compliant Future Internet experiments	If the objective involves risks associated with non-compliance, then yes. Otherwise, no. This goes back to the objective setting up-front.
Improving project design and decision making	The whole essence of the technique is to highlight issues at design time for the decision-makers to make better, and more informed decisions.

Table 10: How useful is Risk Analysis?

Risk analysis does provide some support for the key questions proposed by SESERV. The main emphasis is on highlighting issues, exploring potential solutions, and articulating these to all those with a vested interest, including the decision-makers. It does need to be run iteratively: the technique focuses on a specific objective each time. Additionally, and in contrast to tussle analysis, it is directed towards the (potential) resolution of issues: it is design for a fixed, not a variable outcome. Its strength lies in solution exploration up-front, as well as communication across all involved.

5 Conclusions

The goal to increase participation in political discourse through the use of popular social networking sites has many attractions. Likewise, the goal to comply with data protection legislation is also equally valid and as well as necessary. The social analysis shows that a critical success factor (i.e.

participation) for social networking providers is to maximise activity, which is achieved irrespective of the purpose of the communication between individuals. The risk assessment highlights that for legal compliance providers must take responsibilities (in respect to purpose) and individuals need to take certain actions (e.g. consent). So here lies the contradiction. Privacy compliance, often declared as a way to increase trust, and hence participation, in effect impedes activity and actually acts as an inhibiter to participation. In reality, individuals use social networking sites because their perception of risk is considered low enough for participation. It is the perception of and appetite for risk that that dictate levels of participation, irrespective of associated regulation.

This leads to an interesting challenge for European service providers and research projects such as *WeGov*. How to balance strike the balance between participation and privacy considering desires to monitor and mine data without violating a citizen's right to privacy? Architectures that facilitate communication between individuals regardless of purpose have been important innovators in the Internet. It is a principle that has contributed to the explosion of Internet use (the end-point principle) and it is improbable that the successful paradigms of the last decade, social networking and clouds, would not have prospered if they had considered compliance to the European regulatory environment. Each new paradigm has focused on promoting the benefits of solutions and opted for weak privacy positions. The try it and observe approach has allowed for a privacy balance to evolve over time as participants explored their preferences rather than having them analysed in advance by security experts. Social networking has been in fact a large experiment in people's appetite for privacy.

This paper has considered the challenges faced by an ICT STREP, the *WeGov* project, in this context considering social, economic and regulatory aspects. We looked at a number of analytical techniques, each of which provides a different perspective on the issues that the project needs to address. Figure 4 summarises the analyses in the sections above and should be viewed in connection with Figure 2. Initially, there seemed to be many and varied challenges, some of which might clearly fit within a given domain and some of which seemed to straddle the boundaries between them. Our initial SWOT analysis of *WeGov* homed in on two major concerns: participation and trust. Essentially, how can ordinary citizens be encouraged to take part, whilst at the same time ensuring that they are comfortable with how their input will be used?

With the outcome of the SWOT analysis in mind, the following sections looked at three different perspectives:

1. A social analytical approach, based on collaborative network organisations;
2. Tussle analysis, proposed in connection with network contention; and
3. Risk analysis, which generally looks at the risk (and opportunities) associated with a specific objective.

Each of these approaches revealed and highlighted different issues and challenges. The reworked figure (Figure 4) shows the focus and benefits of a given approach.

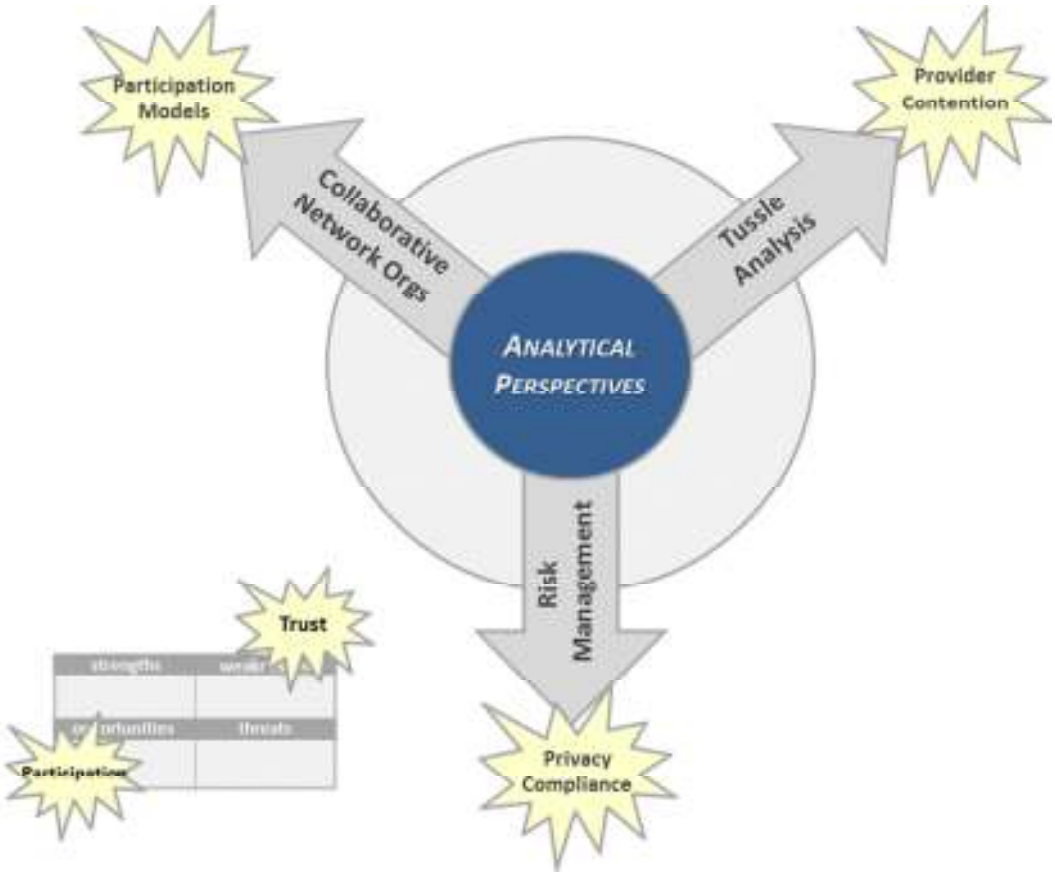

Figure 4: Different perspectives bring varied benefits

The tussle approach concentrates attention for *WeGov* on the contention between the Consortium, wanting to exploit resources, and Cloud providers as well as SNS providers. These are clear economic and resource issues. In other cases, a tussle analysis brought little benefit to the discussion of project challenges. Contention between Government or policy-makers and any of the other stakeholders gained nothing from the approach. In contrast, risk analysis, when focused on the specific issue of data privacy, highlighted much of what would be needed to guarantee compliance to the appropriate legislation. It deals well with regulatory aspects of projects, and helps highlight what might happen and how to mitigate the risk. There was little insight, however, provided for what data protection and trust might mean for those taking part, the general public. Collaborative network organisations (CNO) – the social approach – revealed two significant factors, among many. First: participants in social networks will have their own notions of trust and privacy; as part of a 1.0 Sharing CNO there is an expectation that views and opinions are shared one to many and in the public domain. Secondly, that the consortium, SNS and end-users (government employees) all have some contribution to make to *creating* the processed content needed by policy-makers. They operate within a 3.0 Collaborating CNO, and are subject to different constraints and expectations in terms of the infrastructure required and the implications for the ownership and protection of content. This social analysis focuses on participation, on the one hand between members of the general public (subscribers to the SNS) and on the other between the technologists upon which the *WeGov* deliverables depend. Participatory models are important; regulation and economics have only indirect and secondary significance.

We summarise the approaches attempted above in Table 11. The particular domain of interest (social, economic or regulatory) would seem to dictate the approach to be used. Identifying the most important domain though, in terms of what a project is really about, may not be that easy. The Internet began as a technical challenge to allow technical users (academics) to distribute and share documentation. Routing, data integrity and bandwidth are all important. The Internet has now developed to be a vehicle for social interaction. The focus now, surely, is on its social exploitation than its technical infrastructure.

Methodology	General Approach	Domain	Comments
SWOT Analysis	Analysis of all factors (positive and negative) which might influence a project or activity.	Usually commercially focused.	Provides a rapid means to home in on the major issues: participation and trust. Balance between negative and positive factors is important.
Social analysis	Focus on motivation and issues associated with different modes of interaction.	Social, application layer	Focus is on the real stakeholders (citizens and government-as-beneficiary) and underlines their respective expectations and requirements. As such the problems and issues are set in a different context which refocuses discussion and design into a far more familiar and tractable space.
Tussle analysis	Consider areas of contention; look for stakeholders and analyse the relationship(s) between them.	Economic, technical	Largely a framework to identify that a problem exists; little scope for contention resolution, or the inclusion of factors other than economic/technical.
Risk analysis	Identify risks or issues; examine mitigation possibilities; encourage participation and consensus.	Domain agnostic; useful for consideration of regulatory constraints.	Focus is on problem identification up-front, risk mitigation and participation, at least at the level of knowledge sharing.

Table 11: Overview of analytical techniques to assess the issues for *WeGov*

6 References

1. Bestavros, A (2010) "Tussles in cyberspace", available from http://cs-www.bu.edu/~best/research/talks/TusslesInCyberspace.pdf

2. Brown, I (2010) "Constitutions and tussles in cyberspace", available from http://fi-ghent.fi-week.eu/files/2010/12/1300-5cybercrimegis-1232793782782107-2.pdf

3. Clark, D.D., Wroclawski, J., Sollins, K.R., Braden, R (2002) "Tussles in Cyberspace: Defining Tomorrow's Internet", *SIGCOMM'02,* August 2002, Pittsburgh, Pennsylvania, USA.

4. Dutton, W.H. (2008) "The Wisdom of Collaborative Network Organisations: capturing the Value of Networked Individuals", *Prometheus,* 26:3, 211-230

5. Dutton, W.H. (2010) "Capturing the Value of Networked Individuals: Strategies for Citizen Sourcing", presented at *NETworked Organisations*, organized by SINTEF, at Kanonhallen, Oslo, Norway, 10 November 2010

6. Dutton, W.H. and Shepherd, A. (2003) "Trust in the Internet: The Social Dynamics of Experience Technology", The Oxford Internet Institute, available from: http://www.oii.ox.ac.uk/resources/publications/RR3.pdf

7. Kalogiros, C., Courcoubetis, C., Stamoulis, G.D., Boniface, M., Meyer, E.T., Waldburger, M., Field, D. and Stiller, B. (2011) "An Approach to Investigating Socio-economic Tussles Arising from Building the Future Internet", FIA

8. Koponen, T., Chawla, M., Chun, B-G., Ermolinsky, A., Kim, K.H., Shenker, S. and Stoica, I. (2007) "A Date-Oriented (and Beyond) Network Architecture", *SIGCOMM'07*, August 2007, Kyoto, Japan; available from http://ccr.sigcomm.org/online/files/fp177-koponen1.pdf

9. North, D.W. (1995) "Limitations, definitions, principles and methods of risk analysis" in *Rev.sci.tech.* 14 (4), 913-923

10. The *Risk Management Standard,* (2002) published by AIRMIC, ALARM, IRM. Available for download from those organisations and from: http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

11. Sollins, K.R. (2009) "An Architecture for Network Management", *ReArch'09*, December 2009, Rome, Italy; available from http://conferences.sigcomm.org/co-next/2009/workshops/rearch/papers/Sollins.pdf

12. *Where Government meets the eSociety, WeGov* : http://www.*WeGov*-project.eu/

13. Wold, G.H. and Shriver, R.F. (1997) "Risk Analysis Techniques: The risk analysis process provides the foundation for the entire recovery planning effort" in *Disaster Recovery Journal* http://www.drj.com/new2dr/w3_030.htm

14. Yang, L and Lan, G.Z. (2010) "Internet's impact on expert-citizen interactions in public policymaking – A meta analysis" *Government Information Quarterly 27, 431-441*

15. ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107

16. Expression of Needs and Identification of Security Objectives (EBIOS), http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html

17. Méthode Harmonisée d'Analyse de Risques, MEHARI 2007 Concepts and Mechanisms, CLUSIF, April 2007 https://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2007-concepts_principles_2007.pdf

18. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), http://www.cert.org/octave/

19. Computer Emergency Response Team (CERT), http://www.cert.org

20. *WeGov* D5.1 Scenario definition, advisory board and legal/ethical review http://www.*WeGov*-project.eu/index.php?option=com_processes&task=streamFile&id=11&fid=45