Bridging the Contradictions of Open Data

Ronald Meijer[1], Sunil Choenni[1, 2], Roexsana Sheikh Alibaks[1]and Peter Conradie[2]
[1]Research and Documentation Centre – Ministry of Security and Justice, Den Haag, The Netherlands
[2]Rotterdam University of Applied Sciences – Creating 010, Rotterdam, The Netherlands
r.f.meijer@minvenj.nl
r.choenni@minvenj.nl; r.choenni@hr.nl
r.sheikh.alibaks@minvenj.nl
p.d.conradie@hr.nl

Abstract: For a successful public value strategy, the elements "public values/strategic goals", authorizing environment" and "operational capability" should be coherently aligned. In this paper, we discuss how we have aligned these elements in the context of Open Data. We focus on the relationships between Open Data and public values, in particular, trust, transparency, privacy and security. Several contradictions exist between these values. To succeed, Open Data policy has to reconcile these values. For reconciliation purposes, we introduce the notion of precommitment, which is a restriction of one's choices. Precommitment is conceptualized as a policy-instrument whereby an organization imposes some restraint on its policy in order to restrict the extent to which values may conflict and stakeholders have to worry about the trustworthiness of that policy. We demonstrate how precommitment - implemented as a data request procedure – combined with a proper data infrastructure for Open Data may reconcile potentially conflicting values.

Keywords: open data, trust, privacy, precommitment, data infrastructure

1. Introduction

Open data (OD) is gaining importance in recent years. This increase of importance is taking place in the context of a growing demand for openness. Governments and governmental organizations plead for more openness, e.g. the Obama Administration and the European Union (Zuiderwijk et al. 2012) (Kulk et al. 2012) (ROB 2012). But also the scientific community is calling for more openness with its own research data. Openness is viewed as a means to contribute to transparency and via transparency, it is assumed to contribute to trust of civilians and other stakeholders amongst the government and in science (Zuiderwijk et al. 2012) (Kulk et al. 2012) (ROB 2012) (Schuyt 2012) (Rajamäki 2012). On the other hand, openness may lead to privacy breaches and security violations (Braak, et al. 2012) (Gutmann et al. 2008) (Kalidien et al. 2010) (Kulk et al. 2012).

In line with the increase of the importance of OD, several OD initiatives are going on at the moment (Conradie and Choenni 2012). These OD initiatives all have in common that they are to a certain extent operating with more or less defined goals and objectives, some of which can be categorized as "public value" (PV). The "open" side of OD provides access for the public eye. This clearly underlines the idea that OD is about creating "public" value. OD, as shall be demonstrated in this paper, is not only about creating PV, but also to an important extent, about conserving and maintaining "public values". In fact, an OD policy has to reconcile multiple seemingly conflicting values.

The concept of PV is increasingly popular within both academic and practice settings (Williams and Shearer 2011). Some believe that this concept will be the next "Big Thing" in public management (Talbot 2009). For a successful PV strategy the three elements of Moore's famous "strategic triangle", i.e. "public values/strategic goals", "authorizing environment" and "operational capability" must be brought into coherent alignment (Moore 1995) (Williams and Shearer 2011).

In this paper, we discuss how we have aligned the before-mentioned PV elements for an OD policy in the context of judicial research and registration data at a government research institute. We focus on the relationships between OD and public values, in particular trust, transparency, privacy, and security. Several contradictions exist between these values as will be demonstrated below. In our case, these values form the first of the three strategic triangle elements. The "authorizing environment" in our case is mainly formed by general policy instructions, and privacy laws and regulations. The "operational capability" in our case consists of data infrastructure and staff.

We argue that to be successful, OD policy has to reconcile conflicting values. For this purpose, we exploit the concept of precommitment, which is in essence a restriction of one's choices (Elster 2000; Kurth-Nelson and Redish 2012). We conceptualize precommitment in this paper as a policy-instrument whereby an organization imposes some restraint on its policy in order to restrict the extent to which values may conflict and stakeholders have to worry about the trustworthiness of that policy. Our case demonstrates how by means of a precommitment instrument - implemented as a data request procedure – combined with a proper data infrastructure, OD policy may reconcile potentially conflicting values.

The reminder of this paper is organized as follows. In the next section we start with a condensed description of PV. In section 3 the central "public values" which are encountered by OD policy is described and analyzed. And the concept of precommitment is conceptualized. In section 4 the case of OD policy for judicial research and registration data in a government research institute is presented. In this case solutions for reconciling conflicting public values are presented. Finally, section 5 concludes the paper.

2. Public value approach

The PV framework was originally formulated by Moore (Moore 1995) (Williams and Shearer 2011). PV can best be understood and achieved within the notion of the "public sphere", a democratic space which includes, but is not coterminous with, the state in which citizens address their collective concerns and where individual liberties have to be protected (Benington and Moore 2011). The government is seen as a creator of PV and a pro-active shaper of the public sphere: politically, economically, socially and culturally (Benington and Moore 2011). There is consensus in the literature that PV can be interpreted as combining (and reconciling), safeguarding and enrichment of the public sphere with the delivery of the values that are desired by the public (Williams and Shearer 2011).

Moore's central proposition was "…that public resources should be used to increase value in a way which is analogous to value creation within private enterprise. However, this PV would necessarily extend beyond narrow monetary outcomes to include that which benefits and is valued by the citizenry more generally." (Williams and Shearer 2011). PV is also described as including the value attached to relatively concrete outcomes, and the more intangible (Grimsley and Meehan 2007). The value "trust", which is central to OD, as we shall demonstrate below, repeatedly appears in several definitions (O'Flynn 2007) (Grimsley and Meehan 2007) (Williams and Shearer 2011; p7).

A strategic triangle is central in Moore's PV framework (Williams and Shearer 2011; p5) (O'Flynn 2007). It contains three elements "public values / strategic goals", "authorizing environment" and "operational capability" (Williams and Shearer 2011). For a successful organizational PV strategy, these elements should be coherently aligned. This is attained by complying the strategy to three corresponding broad tests, namely it must be "substantially valuable", "legitimate and politically sustainable" and "operationally and administratively feasible" (Moore; 1995).

For information systems (IS) we find a clear parallel between the PV literature and the literature about the approach of embedding human values in IS. For instance, (Choenni et al. 2011a) stresses on the importance of embedding human values, such as privacy and trust, in the development of information systems. They plead for an explicit agreement with regard to the values that should be included in a design. Thus extending the view about the IS beyond the original more narrowly defined requirements. We argue that "human values" embraced by government become "public values", as they are from then on part of the conditions, goals and objectives of organization strategies. Thus, public managers, adopting a PV approach who aim to create value in IS for e-Government can profit from IS "human value" -design approaches. We also argue that the interpreting of the OD initiatives in the PV paradigm may help to clarify the policy problems which OD may encounter and in doing so may help to raise and increase PV.

3. Public values in open data

OD consists of data that is not identifiable to a person with the aim to be reused and redistributed by everyone, without restrictions from copyright, patents or other mechanisms of control (Zuiderwijk et al. 2012) (LinkedGov 2011) (Open_Knowledge_Foundation 2011) (Sweeney 2009). The idea behind opening public data is to make information that is generated or collected by organizations in the public sector re-usable. This idea is founded on the acknowledgement that citizens are taxpayers and therefore have access rights to this data.

They have this right wherever financially feasible and, when releasing, it won't violate any laws or rights relating to privacy either for citizens or government staff (LinkedGov 2011) (Open_Knowledge_Foundation 2011) (Sweeney 2009).

3.1 Values

Transparency and trust are central values that drive OD. Openness is viewed as a necessary condition for a well-functioning democratic state of law. It serves the legitimacy of Public Administration and the trust of civilians in the government (ROB 2012). The scientific community is also calling for more openness with its own research data. We have observed that in the Netherlands, trust in scientific research is an object of discussion. Regularly, messages that mention cases of questionable research practices appear in the media. A growing distrust against science seems to appear, a distrust which is fed by a series of incidents fully described in the media (Schuyt 2012). Several cases of fraud have been discovered in recent years (Heilbron 2005). The proposed measures point to more openness and transparency. Besides good data management, peer pressure, archiving and sharing is advocated. These elements support the replication of research. As a consequence the chances of fraud decrease, while the chances of discovering fraud increase (Schuyt 2012). Therefore we argue that openness contributes to transparency and via transparency, it contributes to trust of civilians and other stakeholders, amongst the government and in science (Zuiderwijk et al. 2012) (Kulk et al. 2012) (ROB 2012) (Schuyt 2012) (Rajamäki et al. 2012).

The IS evaluation framework based on PV of Grimsley and Meehan (2007) focuses upon citizens' and clients' experiences of service provision and service outcomes as contributors to the formation of public trust. They show that trust is related to the extent to which people feel that an e-Government service enhances their sense of being well informed, gives them greater personal control and provides them with a sense of influence or contingency (Grimsley and Meehan 2007). In the context of law enforcement Rajamäki et al. note that people feel they have lost control over their own data and they do not know who handles personal data, when and for what purpose. This concern can be answered by increasing transparency of these operations (Rajamäki et al. 2012). The principle of transparency is that information should be shared while data is collected. Possibilities for control must be created and people assured that there is no abuse (Rajamäki et al. 2012). As will be argued in section 3c, constraints imposed on the access to data therefore are important for trust: in deciding how far one party needs to trust the other and vice versa. Transparency is also important for trust as by transparency the unilateral restraints imposed can be verified by the stakeholders.

As described above, OD refers to data that does not reveal personal identity. We argue that privacy is thus another central PV in OD. By means of the Data Protection Directive the European Union requires that if personal data is processed, this should be done fairly, lawfully and for specified, explicit and legitimate purposes (Article 6 of the Data Protection Directive). The purposes for which the data is processed must be explicit and legitimate and must be determined at the time of collection of the data (Recital 28 of the Data Protection Directive) (Kulk et.al. 2012). In the Netherlands important principles of justice are anchored in the Dutch Privacy Protection Act (DPPA), such as finality, legitimacy, proportionality and subsidiarity, transparency and data subject's rights. Finality refers to the purpose for which personal data is collected. This purpose should be explicit and the processing of collected data must be compatible with the purpose for which they were collected. Legitimacy refers to the process of data collection and also to the context of the data: data must be processed in a proper, careful, and legal manner. Moreover data must be relevant, sufficient, not excessive, and correct (Versmissen 2001). Proportionality demands that the means used are proportional to the intended purpose. Subsidiarity demands the use of the alternative which minimizes the use of privacy sensitive data. Transparency refers to the right that the data subject is entitled to know if someone is processing data about him. The data processing party has the obligation to identify itself to the data subject and has to inform him about what data it processes and the purposes of processing (Versmissen 2001).

The fourth and final OD value we discern in this paper is security. Security is a comprehensive notion. However, we derive this value from the privacy value. To prevent accidental or malicious disclosure, modification, or destruction of records and data sets, data security is indispensable (Denning and Denning 1979). Research and registration databases may contain privacy sensitive data. The opening of this data therefore should be done in strict compliance with the privacy value to prevent privacy breaches. In other words the security of the data has to be protected. In section b below, we will go into more detail on this value.

3.2 Analyzing values

Having identified the values playing a crucial role in OD, here we analyze how they are related to each other. Figure 1 resumes the OD values as described above. It depicts the public OD values transparency, trust, privacy and security and the way they assumingly relate to each other and to three selected intermediary elements, replicability, information overload and reliability. The way public values and intermediary elements relate to each other is depicted by arrows. These elements may reinforce each other, indicated by a "+"sign, or contradict, "-"sign. The intention of this chart is not to be complete. Its intention is to show the apparent contradictions between the public values on which we focus in this paper. The intermediary elements will only be briefly described in relation to the values. An elaborate discussion of these elements is beyond the scope of this paper.

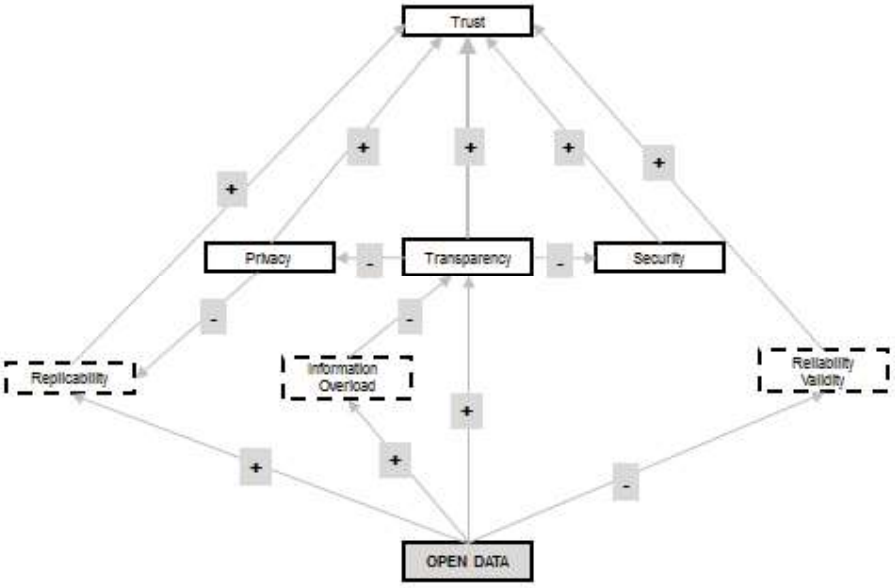

Figure 1: Open data values

OD - making data accessible for (re-)use to the public – is assumed to contribute to transparency. By giving access to research and (semi)government data, civilians, policy makers, journalist, audits and scientists get opportunities to control, verify the data, replicate research findings or create new findings. It is assumed that this results in maintaining or increasing trust. However there is a "dark side" to opening data without constraints or restrictions imposed on the access to data. This "dark side" may lead to several contradictions in the OD policy values.

In the first place OD may conflict with privacy. The opening of data is seriously impeded when privacy sensitive data are at stake. OD may not seem to be personal data at first glance, especially when it is anonymized or aggregated. However, it may become personal data by combining it with other publicly available data or when it is deanonymized (Kulk et al. 2012) (Denning and Denning 1979). Anonymizing data cannot be "100% privacy proof". Even when data with a high aggregation level is shared, the risk that one is able to deduce or abduce privacy-sensitive information remains (Braak et al. 2012) (Ohm 2009). Opening up data without taking into account the privacy risks attached, may lead to privacy breaches with possibly very negative consequences for the trust of respondents who participated in research and civilians in research or government. We may have found a possible negative relation between the privacy value and trust. To prevent privacy breaches, it is necessary to eliminate privacy sensitive attributes. However this may have a negative impact on the possibility of using the OD for replicability as some of the attributes needed to ensure the replication cannot be used any longer. Thus as privacy is protected, not all results may be replicated as a consequence. This may have negative impact on trust.

Next, OD may conflict with security, the principal goal in which the government research institute of our case is operating. Identity disclosure from survey or administrative data might be used by private or public groups to target or harm individuals, population subgroups, or business enterprises (Gutmann et al. 2008). Privacy of civilians thus needs to be thoroughly protected. Civilians expect that public organizations follow rules and procedures carefully in order to protect them and their privacy. Civilians that are harmed due to incorrectly followed rules and procedures may cause social unrest. Therefore, measures to enforce that rules and procedures are followed correctly should be taken into account while developing infrastructures for data sharing in the public domain (Braak et al. 2012).

Thirdly, OD may conflict with transparency, via the intermediary element information overload. In the literature we find that information overload occurs when information received becomes a hindrance rather than becoming potentially useful (Bawden 1999). Information overload is related to the quantity and diversity of information available (Bawden 2009). We therefore argue that as governmental organizations possess large volumes of data about many subjects the opening up of this data may cause information overload.

Finally, OD may have negative effects on trust via the intermediary element validity and reliability of the results in cases where the data is re-used. This may concern re-use on the basis of the data provided but also on the basis of extension of data with other (open) data sources. We argue that as data are opened the governmental control on reliability and validity decreases due to a possible lack of a proper interpretation. Third parties may use the opened data in ways that weaken these elements. Data from administrative databases might for instance be misinterpreted and misused with the stigmatization of groups as a consequence (Kalidien et al. 2010).

3.3 Precommitment

We have found several contradictions between the OD values. Consequently, to succeed, OD policy has to reconcile these values. We argue that constraint imposed on the access to data is important for trust: in deciding how far one party needs to trust the other and vice versa. We argue that precommitment is necessary to bridge the contradictions in OD.

Precommitment is a restriction of one's choices (Elster 2000) (Kurth-Nelson and Redish 2012). It is implying constraint. Individuals might benefit from having specific options unavailable, available only with a delay, or at greater cost. Precommitment may be aimed at overcoming impulsivity (e.g. in gambling machines require the gambler to pre-set a limit on his or her expenditure, after which the machine deactivates (Kurth-Nelson and Redish 2012). Precommitment is also theorized as a device whereby we can impose some restraint on ourselves and thus restrict the extent to which others have to worry about our trustworthiness (Gambetta et al. 2000).

We conceptualize precommitment as a policy-instrument whereby an organization – in case responsible for OD - imposes some restraint on its policy in order to restrict the extent to which values may conflict and stakeholders have to worry about the trustworthiness of that policy. To limit possible conflicts between OD values several restraining options for opening data are possible. In the first place privacy sensitive data might be irrevocably deleted. Datasets may be completely anonymized before they are archived, thus limiting the future possibilities to replicate research or to link the datasets to other data to create new datasets. Secondly, data including privacy sensitive attributes might be opened for specific goals or target groups only. Some data (e.g. registry databases of police and prosecution) might only be distributed for specific scientific purposes and to scientific institutes only – in compliance with privacy laws and regulations in vigor. Thirdly, before the opening of data from research to public, all privacy sensitive data needs to be thoroughly removed. As a result the opened datasets will contain only limited information and can be analyzed only in a (very) restricted way. Finally, data can be made accessible in an indirect way by the provision of exclusively highly aggregated data only. These data is generated by data experts.

The following case illustrates how precommitment is implemented in the open data policy of a government research institute operating in the field of security and justice.

4. A case: Open data policy of a Government research institute

At the Research and Documentation Centre of the Ministry of Security and Justice - in Dutch "Wetenschappelijk Onderzoek- en Documentatiecentrum" (WODC) - data is gathered to advise about and to define the current and future research agenda of the Dutch Ministry of Security and Justice, to answer policy-related questions and to indicate the possible implications of research findings for standing policy. For this purpose WODC systematically collects, stores, enhances and provides criminal justice information produced by themselves or external organizations commissioned by WODC (Zuiderwijk et al. 2012).

WODC strives towards transparency, thus investing in trust, while giving priority to protecting privacy. WODC aims to facilitate the reuse of research data, as this may provide the organization with benefits, such as the possibility to scrutinize and validate the data and to decrease the workload of the WODC. WODC works with confidential judicial research and registration data, so that issues as confidentiality and privacy-sensitivity should be thoroughly taken into account (Zuiderwijk et al. 2012) (Kalidien et al. 2010). WODC therefore has developed a procedure to share data from the collected data as much as possible with other parties, while protecting privacy and in compliance with the restrictions of the privacy protection principles and laws. This procedure is combined with a data infrastructure to manage the contradictions of different values. In two consecutive sections we discuss data infrastructure and -procedure.

4.1 Data infrastructure

Data from concluded research projects is collected. Data from those projects that is qualifying for public opening is centrally stored in compliance with the Dutch Privacy Protection Act (DPPA). Privacy sensitive data is deleted unless explicitly needed for further research (longitudinal research, monitoring projects). Public safety registration data is stored in a data warehouse (DW), containing police and justice data, for policy research purposes. A DW ensures a uniform approach to data for interpretation purposes and ensures maximum accessibility. Privacy is protected as the DW is anonymized, i.e. has been stripped of directly identifying attributes, like names, addresses etc. In the DW problems around inconsistencies, reliability, and validity are tackled (Choenni and Meijer 2011b). The archived research data and DW data form the basis of the WODC data request policy.

WODC may decide to the public opening of research data. The research data of WODC is open for everyone once - contented to the high criteria of DPPA and confidentiality matters – it is uploaded on the server of the Dutch Archiving and Networked Services (DANS). Before opening the data from research to public, all privacy sensitive data – which may lead to disclosure directly as well as indirectly - is removed. WODC may permit restricted access to scientific organizations for scientific purposes to privacy sensitive research data. The DPPA allows the (re-) use of personal or privacy sensitive judicial data, under certain conditions, for scientific purposes. Public safety registration data might be released only for scientific research to scientific organizations. WODC regularly receives individual data requests from scientists for permission to re-use research data or for an extract of public safety data from the DW. Extracts from the DW may – in principle – be opened, but for scientific research only. WODC gives access to the data by providing highly aggregated data on demand. This data is generated by data experts and concern DW data requests mostly.
Each and any request is thoroughly audited by the WODC data request procedure.

4.2 Procedure

The data request procedure is a rigorous procedure which is aimed at sharing data with other parties as much as possible, while thoroughly protecting privacy. With the aid of this procedure we manage to protect privacy sensitive attributes in datasets, in compliance with the security policies.

WODC discerns two subtypes of data requests to contribute to OD and give access to citizens, namely requests for Statistical Information and requests for Data Supply. Statistical Information is aggregated data on which people do not aim to edit the data information. This information can be based on registration as well as research data of WODC. The output provides a minimal opportunity to be edited. Data supply can be subdivided in requests for re-use of research data from published research or requests for an extract of registration data from the data warehouse (DW).

WODC distinguishes three steps towards the opening of data while protecting privacy. At first an experienced data manager carefully studies a data request to see which variables are necessary for an applicant, whether the required variables could be delivered from the centrally archived research data or the DW. The data manager prepares a preliminary decision to a request by making a report with considerations such as legal requirements, policy sensitivity and quantity of work for WODC. This document is sent to the workgroup of DPPA asking them to exam the legal conditions of the request. The data request is tested on the criteria of the DPPA by the workgroup. In this phase every kind of convertible (personal) facts not in agreement with privacy laws and rules are removed. When necessary a Trusted Third Party is included in the data request project, in order to prevent the unnecessary transfer of privacy sensitive data (Braak et al. 2012). The subsequent and final stage is the judgment of the board of directors. Board members discuss the request looking at the advice written by the data manager (based on their experience and comments of the DPPA workgroup) and decide whether or not the data should be delivered to the requested party and on which conditions. An appraisal of the board of directors leads to delivering data after signing a standard agreement and specific conditions of reuse by the applicant.

5. Conclusion

We have observed a relationship between OD and public values. This relationship is described by the values trust, transparency, privacy, and security. As we have argued, several contradictions between these values exist. To solve these contradictions we have introduced the notion of precommitment: a policy-instrument whereby an organization imposes some restraint on its policy in order to restrict the extent to which values may conflict and stakeholders have to worry about the trustworthiness of that policy. We have elaborated this notion in a rigorous data request procedure. To manage the contradictions between values we combine this procedure with a data infrastructure. By means of the WODC case, we have illustrated how contradictions are handled.

The case illustrates how the priority to protect privacy on the one hand leads to the limitation of the opening of data to the public, but on the other hand gives the opportunity to OD in a restricted mode for scientific goals. A DW assures reliability of answers to statistical information requests. Hereby privacy is protected by presenting only very highly aggregated data to the general public. Requests for data supply mostly concern data on the level of unique identifying records in research datasets or registration data. Therefore in these type of requests most of the time, privacy sensitive data is involved. In these cases data is supplied only for scientific goals in compliance with the privacy laws and regulations. Moreover, by verifying the data on legal and policy confidentiality points of views on several moments in different phases, the chance of failure is reduced to a minimum, thus maintaining trust. Opening data to scientists creates possibilities to re-use and (partly) replicate existing research findings, thereby contributing to trust.

Acknowledgements

The authors wish to thank Rochelle Choenni for her valuable contribution to this paper, in particular for verifying the final version on correct and fluent English.

References

Bawden, D. and Robinson, L. (2009) The dark side of information: overload, anxiety and other paradoxes and pathologies, *Journal of Information Science*, Vol 35, No. 2, pp. 180-191.

Bawden, D., Holtham, C. and Courtney, N. (1999). Perspectives on information overload, *Aslib Proceedings*, Vol 51, No. 8, pp. 249–255.

Benington, J. and Moore, M. (2011) Public Value: Theory and Practice, Palgrave Macmillan, Basingstoke.

Braak, S.W. van den, Choenni, S., Meijer, R. and Zuiderwijk, A. (2012) "Trusted third parties for secure and privacy-preserving data integration and sharing in the public sector," in Proceedings of the 13th Annual International Conference on Digital Government Research, New York, NY, USA, 2012, pp. 135-144.

Burns, N., and Grove, S.K. (2001) *The practice of nursing research: Conduct, critique & utilization* (4th ed.). Philadelphia: Saunders.

Choenni, R., Waart, P. van, and Haan, G. de (2011a) Embedding Human Values into Information System Engineering Methodologies, Proc. ECIME 2011, 5th European Conf. On Information Management and Evaluation, Como, Italy, Sept. 8-9, Academic Publishing Limited, UK, pp. 101-108.

Choenni, S. and Meijer, R. (2011b) From Police and Judicial Databases to an Offender-Oriented Data Warehouse, IADIS International Conference e-Society 2011, 10-13 march, Avila, Spain.

Conradie, P. and Choenni, S. (2012) "Exploring Process Barriers to Release Public Sector Information in Local Government," in 6th International Conference on Theory and Practice of Electronic Governance, Albany. NY. Albany, New York, pp. 5-13.

Denning, D. E. and Denning, P. J. (1979) Data Security, *ACM Computing Surveys*, Vpl. II, No. 3.

Elster, J. (2000) Ulysses Unbound: Studies in Rationality, Precommitment, and Constraints. Cambridge University Press.

Gambetta, D. (2000). "Can We Trust Trust?", in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology,University of Oxford, chapter 13, pp. 213-237.

Grimsley, M. and Meehan, A. (2007) e-Government systems: evaluation-led design for public value and trust. *European Journal of Information Systems*, Vol 16, pp. 134-148.

Gutmann, M., Witkowski, K., Colyer, C., O'Rourke, J. and McNally, J. (2008) Providing Spatial Data for Secondary Analysis: Issues and Current Practices Relating to Confidentiality. *Population Research and Policy Review*, Vol 27, No. 6, pp. 639-665.

Heilbron, J. (2005) *Wetenschappelijk onderzoek: dilemma's en verleidingen*, KNAW, Amsterdam.

Itani, W., Kayssi, A. and Chehab, A. (2009) "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," in Proc. 8th IEEE Int. Conf. on Dependable, Autonomic and Secure Comput., Chengdu, China, 2009, pp.711-716.

Kalidien, S., Choenni, S. and Meijer, R. (2010) Crime Statistics On Line: Potentials and Challenges, in: Public Administration Online: Challenges and Opportunities, proceedings of the 11th Annual International Conference on Digital Government Research, DG. O 2010, Puebla, Mexico, May 17-20, ed. by S.A. chun, R. Sandoval and A. Philpot ACM Press, Digital Government Research Center, 2010, pp. 131-137.

Kamensky, J.M, (2009) "Making Sense from Information Overload Governments need to apply the science of analytics to the vast amount of data they collect", (online), Governing. Management Insights. http://www.governing.com/columns/mgmt-insights/Making-Sense-from-Information.html

Kulk, S. and van Loenen, B. (2012) Brave New Open Data World?, *International Journal of Spatial Data Infrastructures.* Vol 7, pp.196-206.

Kurth-Nelson, Z. and Redish, A. (2012) Don't Let Me Do That! – Models of Precommitment. *Front Neurosci.* 2012; 6: 138. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3465853/

Langheinrich, M. (2001) "Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems," in Gregory D. Abowd, Barry Brumitt, Steven A. Shafer (Eds.): Proceedings of the Third International Conference on Ubiquitous Computing (UbiComp 2001). LNCS No. 2201, Springer-Verlag, pp. 273-291, Atlanta, USA, 2001.

Levelt, W.J.M. (2012) "Falende wetenschap: De frauduleuze onderzoekspraktijken van sociaal-psycholoog Diederik Stapel"(online), Tilburg University, www.foliaweb.nl/wp-content/.../2012/11/Eindrapport-definitief-16nov.pdf

LinkedGov. (2011) "What is Open Data?",(online), Retrieved December 8, 2011, from http://linkedgov.org/what-isopen-data/

Moore, M. (1995) *Creating Public Value: Strategic Management in Government*. Cambridge, Massachusetts: Harvard University Press.

O'Flynn, J. (2007) 'From New Public Management to Public Value: Paradigmatic Change and Managerial Implications', *Australian Journal of Public Administration*, Vol 66, No. 3, pp. 353-366.

O'Flynn, J. (2005) A Public Value Framework for Contractual Governance, *PUBLIC*, Issue 07, ESADE Institute of Public Management, Barcelona, December (invited contribution).

Ohm, P. (2009) *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,* Social Science Research Network. Vol 57, No. 6 , pp. 1-64.

Open_Knowledge_Foundation. (2011). What is open? Retrieved December 8, 2011, from http://opendatamanual.org/what-is-open-data/what-is-open-data.html

Rajamäki, J., Tervahartiala, J., Tervola, S., Johansson, S., Ovaska, L. and Rathod, P. (2012) How Transparency Improves the Control of Law Enforcement Authorities' Activities? EISIC, pp. 14-21. IEEE Computer Society 2012.

ROB, De Raad voor het openbaar bestuur (2012) "Gij zult openbaar maken: Naar een volwassen omgang met overheidsinformatie"(online), http://www.rob-rfv.nl/documenten/boekje_advies_openbaarheid.pdf

Schuyt, C.J.M. (2012) *Zorgvuldig en integer omgaan met wetenschappelijke onderzoeksgegevens, Advies van de KNAW-commissie onderzoeksgegevens.* Amsterdam, 2012.

Stanberry, B. (1998) The legal and ethical aspects of telemedicine. 2: Data protection, security and European law. J Telemed Telecare. 1998. Vol 4, No. 1, pp. 18-24.

Sweeney, K. (2009). *Open Data: Meaning, context and implications.*

Talbot, C. (2009) Public Value - The Next "Big Thing" in Public Management?, *International Journal of Public*, Administration, Vol 32, No. 3-4, pp. 167-170.

Versmissen, J.A.G. (2001) *Achtergrondstudies en Verkenningen. Sleutels van vertrouwen van vertrouwen TTP'S digitale certificaten en privacy*. Registratiekamer, Den Haag.

Williams, I. and Shearer, H. (2011) Appraising Public Value: past, present and futures. *Public Administration*, Vol 89, No. 4, pp.1367-1384.

Zuiderwijk, A., Janssen, M., Meijer, R., Choenni, S., Charalabidis, Y. and Jeffery, K. (2012) Issues and Guiding Principles for Opening Governmental Judicial Research Data. Proc. EGOV 2012, 11 th European Conf. On Electronic Government, Kristiansand, Norway, September 3-6, LNCS, Springer verlag, Germany, pp. 90-102.