Privacy and Information Sharing in a Judicial Setting: A Wicked Problem

Mortaza S. Bargh
Research & Documentation Center
Ministry of Security and Justice
The Hague, The Netherlands
m.shoae.bargh@minvej.nl

Sunil Choenni[1, 2]
[1]Research & Documentation Center
Ministry of Security and Justice
The Hague, The Netherlands
r.choenni@minvenj.nl
[2]Creating 010
Rotterdam Uni. of Applied Sciences
Rotterdam, The Netherlands
r.choenni@hr.nl

Ronald Meijer
Research & Documentation Center
Ministry of Security and Justice
The Hague, The Netherlands
r.f.meijer@minvenj.nl

ABSTRACT
Information sharing has become a means of gaining public trust for institutions such as governmental and scientific organizations. The transparency sought through information sharing contributes to the trust of various stakeholders such as citizens, other organizations and enterprises in such institutions. Information sharing, on the other hand, may increase the chance of privacy breaches due to, for example, information leakage and information fusion. Such privacy breaches can undermine stakeholders' trust and thus work against the purpose of gaining trust through transparency. Moreover, fear of potential privacy breaches compels information disseminators to share minimum or no information. In this contribution we show that creating transparency through sharing information in the context of our public judiciary organization is a typical wicked problem. Subsequently we explain (the outcomes of) our designerly approach to design and intervene three artifacts within our organization. These artifacts are aimed at disseminating our judiciary data in a privacy preserving way, as privacy preservation contributes positively to the information sharing. Through addressing the privacy problem we try to address the transparency problem.

Categories and Subject Descriptors
K.4.1 [**Computing and Society**]: Public Policy Issues – *Privacy, regulation, transborder data flow*.

General Terms
Design, Security, Human Factors, Legal Aspects.

Keywords
e-Government, feedback, information sharing, privacy, transparency

dg.o 2015, May 27 - 30, 2015, Phoenix, AZ, USA
© 2015 ACM. ISBN 978-1-4503-3600-0/15/05…$15.00
DOI: http://dx.doi.org/10.1145/2757401.2757425

1. INTRODUCTION
Governmental and scientific institutions have sought for transparency through sharing their data in order to gain the trust of citizens, organizations and enterprises [21][30][31][39] (or as Bertot et al. put it: "transparency and the right to access government information are now internationally regarded as essential to many functions of democracy: participation, trust in government, prevention of corruption, informed decision making, the accuracy of government information, and provision of information to the public, companies, and journalists, among other essential functions in society" [5]). Steadily information sharing gains more importance as a result of growing demand for openness and transparency in recent years. Information sharing, on the other hand, may create various side effects or may be affected by other problems such as data misuse, data misinterpretation, and personal data compromise. In this contribution we limit our scope to the privacy problem, which is intertwined with data dissemination and thus with transparency.

Information systems that process, e.g., collect, enhance, store, and share, privacy sensitive information (like names, email and postal addresses, dates of birth, geo-locations, bank account numbers, photos and political/personal opinions) are fairly vulnerable to information leakage and thus to privacy breaches [2]. This information leakage stems from, for example, cyber attacks, compromised systems, or (un)intentional disclosure of privacy-sensitive information through fusing the information with the information of other sources. Although numerous privacy enhancing technologies such as data anonymization (suppression, aggregation, and abstraction), pseudonymization and perturbation [27] are used to remove personal identification information, the resulting data may become personal when one combines it with other available data or when one de-anonymizes the data [7][21].

Privacy breaches can have negative consequences for trust in the guardians or controllers of the private information (e.g., scientific or governmental institutions). Not only is the trust in such organizations on stake, there are also enormous costs inflicted on individuals, businesses and the society at large if privacy is compromised. Individuals (i.e., data subjects like citizens) can face various risks such as emotional embarrassment, loss of employment/business opportunities, increased health and life insurance fees, and identity theft. For organizations and businesses the costs of data breaches range from direct costs (such as legislative fines, shareholder lawsuits, third party and customer

compensations, profit loss, legal defense costs) to indirect costs (such as those for upgrading and maintaining of protective systems and safeguards), and implicit costs (such as those associated with reputation and branding damages, loss of goodwill, affected turnover and customer loyalty). Privacy breaches impact also the society at large because the breaches diminish the collective trust of people in online services, upon which the foundation of our current networked society rests.

Transparency through information sharing aims at gaining the trust of the public and citizens in governmental and scientific institutions. Sharing data, on the other hand, might lead to an increased chance of privacy breaches, which diminishes the intended trust of the public and citizens. Transparency via sharing data, as a result, becomes a typical wicked problem that is often addressed by a designerly approach [38]. (The concept of designerly is articulated by N. Cross, see [14] and the references therein.) In this contribution we use the ten criteria of Rittel and Webber [33] for wicked problems to show that creating transparency through information dissemination can be characterized as a wicked problem in the context of our public judiciary organization.

Subsequently we elaborate on our designerly approach (i.e., through some designed interventions) to address the privacy problem that contributes negatively to information sharing (thus, to the transparency problem). Therefore, our objective in this contribution can be described as how to accommodate transparency and privacy-preservation in information sharing within the context of our judiciary organization. The ultimate objective, in turn, is to enhance the trust of the public and individuals in governmental institutions. Specifically, the paper reports on the main results achieved through design and intervention of three artifacts: a restricted access procedure, an open access procedure, and a mashups tool to share our judicial information with employees and individuals from, within, and outside of our organization. In this contribution we elaborate on how the problem (and solution) space has evolved during the study. Note that, to this end, we do not intend to describe the details on design options and decisions due to space limitations.

The distinctive characteristics of this study are its reality (i.e., applied to the Dutch Ministry of Security and Justice with real judicial data of citizens), longevity (i.e., ongoing for almost a decade), continuity (i.e., carried out in overlapping phases), flexibility (i.e., adapting to the changing environmental conditions, given the long temporal span of the study), and complexity (i.e., making hard decisions to accommodate privacy and transparency within different contextual settings and organizational constraints). Our three artifacts are good-enough solutions (i.e., we did not intend to seek for most comprehensive, complete and optimum/optimized solutions), given the objectives, the constraints and the context. Within our study we have used feedback mechanisms to inform data controllers about how their data is used. Embedding feedback mechanisms encourages data controllers to share more information, enables them to better examine the context of data sharing, and provides them with more control on their privacy concerns even when the data resides on external system nodes.

In the next section we outline the organizational setting within which the study has taken place. In Section 3 we provide some background information about privacy and describe why transparency via information sharing is a typical wicked problem in our setting. In Section 4 we present an overview of our three designed interventions to indicate how the problem (and solution) space has evolved during the study. In Section 5 we discuss the results attained and in Section 6 we draw some conclusions.

2. SETTING AND APPROACH

Here we describe the judiciary organization the shares information for transparency purposes. We provide also the strategy of the organization for scientific research, which governs (and determines the framework for) our design decisions.

2.1 Organization

The research and documentation center (or Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) in Dutch) is the research center of the Dutch Ministry of Security and Justice. The WODC systematically collects, stores and enhances the Dutch judicial information directly or indirectly through its external partner organizations. The resulting criminal-justice information is used to define the future research agenda, to answer the policy-related questions, and to assess the possible implications of standing policies of the ministry. The WODC, hereon to be referred to as the 'research center', also strives for openness and transparency through knowledge sharing and utilization of its data. Sharing data without taking into account and without taking measures against privacy risks may lead to privacy breaches with negative consequences for trust in the organizations that share the data. The research center, therefore, considers it very important to deal with any negative side effects that this information sharing may bring, particularly about privacy breaches and misinterpretation or misuse of data.

2.2 Strategy

With the arrival of a new department head in 2005, an explicit long-term strategy was formulated for the research center's data sharing activities in order to achieve openness and transparency. This strategy possesses four properties of being: demand-driven, sustainable, feasible, and research-oriented.

The strategy keeps an open eye for the demands and wishes of the stakeholders with regard to information sharing. For complex or time consuming demands and wishes, we assess the feasibility of objectives, given the resources/expertise available at the center. At the same time, we assess whether the knowledge obtained by addressing a demand can also be used in other projects in the near future, i.e., whether the efforts of addressing such a demand can be sustainable. Sustainability refers to the research center's demand-driven activities that will be relevant for a long term, e.g., about 5 years or longer, or that can be retargeted to new upcoming demands. Finally, addressing a demand should involve a research component and should have enough scientific challenges. Figure 1 illustrates the four characteristics of our strategy schematically, where we keep an open eye along the four dimensions of being demand-driven, sustainable, feasible, and research-oriented.

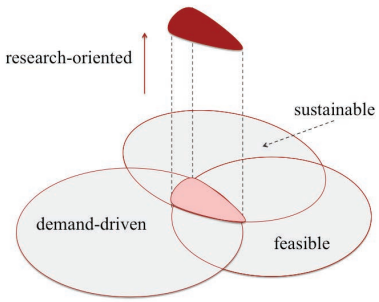

Figure 1. An illustration of the characteristics of the strategy.

Those projects that have a good assessment on all these dimensions become eligible to be carried out within the research center. The department head, often in cooperation with the director of the research center, makes these four assessments. They may consult some domain experts who are more familiar with those topics relevant for addressing the demand. If the department head is confident that the researchers at the research center, possibly in cooperation with other institutes, can successfully handle the scientific challenges, a project proposal is presented to the management team of the center for approval.

The rationale behind our strategy is to serve our stakeholders and increase our research center's viability. On the one hand, we should be able to manage our stakeholders' expectations by carrying out those feasible projects that meet their real demands. On the other hand, we should carry out those projects that are sustainable (i.e. relevant for a long term), thus hereby to contribute to the viability of our institute. The rationale behind carrying out projects with scientific challenges is that, on the one hand, we are able to identify those new/unknown challenges that are relevant for our stakeholders. Even if we are not equipped to tackle these (new) challenges alone, e.g., those challenges that are fundamental in nature, we can identify and communicate these challenges to the scientific world. On the other hand, through research we can acquire new knowledge and expertise, which might be useful within future projects. Furthermore, we could hereby contribute to the state of the art scientifically. Both aspects (i.e., identifying new challenges and acquiring new knowledge) increase our center's viability.

The wishes and demands of stakeholders determine the problem setting of our innovative projects. For a problem at hand, particularly, we seek a feasible solution that is sustainable. Actually, we build on the insights that we have acquired in the past in executing our projects. As a consequence, this strategy reduces the design options since feasibility implies that we should rely on and use the available expertise and resources. Therefore, those design options that require the knowledge and expertise that is unavailable at our research center or takes a significant amount of time, costs and efforts to acquire will not be eligible. We are aware of the fact that, as a consequence of the chosen strategy, we may miss those design options that are better suited for a problem at hand. When, nevertheless, we see that we might miss excellent design options, we start a number of pilot projects to acquire the new knowledge, expertise and experiences. For example, in 2010 we had foreseen a call for open data by our stakeholders. Thus, we started a number of pilot projects in the field of Open Data in 2010. These projects were aligned to the projects in the research direction of information sharing at our research center.

3. BACKGROUND

In order to address the problem of transparency through information sharing we have mainly focused on addressing the privacy issue that contributes negatively to the information sharing. Therefore this section first provides some background information on privacy (preservation) and subsequently explains the rationale behind the wickedness of the problem of information sharing within our judiciary setting.

3.1 Privacy

Privacy possesses many facets, which makes it difficult to provide a unique definition of privacy [12]. Conger and Landry [12] enumerate a number of characteristics of privacy like: anonymity, fair use, controlled access, and use for integration. The anonymity characteristic implies that the data has no relation to a specific entity like a user, group or organization. There are many anonymization technologies like suppression, aggregation, and abstraction to remove the unique distinguishability of an entity from the data under consideration. Fair use is another characteristic of privacy that includes aspects like limited data collection/usage in a given context and no sharing of data without the consent of the data owner. The controlled access characteristic governs the way (e.g., how far and to whom) the information can be moved across physical and organizational boundaries, i.e., data in transit. The use for integration encompasses practices such as integration, profiling and resale of privacy sensitive information.

We in this paper adopt a common definition of information privacy, given by Westin in 1967, which is: "privacy is the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others" [12][29]. Westin's definition of privacy "focuses on information access: how information comes to be known" [17] or, in other words, the definition is concerned with access control. We also adopt this definition because it fairly captures the concept of privacy in our information sharing setting and the way in which we have operationalized privacy preservation in our study. Our realization of privacy preservation mainly relies on giving access to data based on the context of information sharing and based on the content of the shared information. These two pillars are well captured in the abovementioned definition (i.e., the terms "information", "when", "how", and "to what extent").

Privacy is also about knowing how far to share information in an appropriate way in a given context. In the access control model, this 'knowledge' is prerequisite to grant or deny the access. Nissenbaum [26] considers "contextual integrity" as the benchmark of privacy. According to [26] privacy is infringed when one or more "information norms" are violated in a given situation. These information norms are of two types: appropriateness, which governs what information about persons is appropriate to reveal in a given context, and flow or distribution, which governs how far information about persons is transferred in a given context. The context here is a sphere in which the information is shared (e.g., location, politics, convention, cultural expectation, etc.) and it captures the whole environment including the audience [26].

In the era of distributed and interconnected systems like Internet, preserving privacy extends beyond the boundaries of access control that only prevents unauthorized data access at a given moment (i.e., the moment after every data request). The privacy problem arises when personal information is shared with or used by data processing services out of the context for which the data is collected [6]. For example, given a perceived context, individuals share their personal information in social networks to gain friendship, support, recognition, knowledge, etc. [6]. Privacy issues may arise, when the shared information is used for advertisement purposes. Nowadays it is easy to copy, aggregate and fuse information, and eventually infer sensitive private information from publicly available information sources in the Internet. As such, usage control, where the focus lies on how data is used, gains more importance steadily [17][11]. O'Hara [27] calls this usage control as "anonymity model" where one feels private if freely available information cannot be linked to individuals. In addition O'Hara recognizes the traditional "control model" where one feels private if accessing his/her information is controlled by him/her. According to [27] the anonymity model predominates the attitude of younger people while the control model predominates the attitude of older people. Also in the usage control model, it is necessary to 'know' how the data is used.

Although the current work does not focus on the usage control aspect of privacy, our work touches slightly upon 'knowing' (i.e., monitoring) and 'providing feedback' about how personal information is being used.

3.2 Wicked problem

One can use modeling techniques to enhance the reliability and robustness of an information system. Tschantz and Wing [36] mention that privacy modeling of information systems is challenging, even more than security modeling of such systems. They argue that in security you need to model a system, adversaries and the interactions between them. For modeling privacy, however, you need to consider the data subject (and/or data owner) in addition to the system (acting as a data controller and/or a data processor) and adversaries (who are part of the environment). The extra twist in privacy settings mainly stems from subjectivity and extra context-dependency of privacy as mentioned above. A data subject under different contextual situations decides differently about revealing her/his privacy information. For example, a user becomes happy when the system reveals her/his location in an emergency situation, while she/he often does not want the system to reveal her/his location at all. As another example, patients would like to share their medical records with medical personnel for diagnostic purposes but do not want to share this information with health insurance advisors.

Another hurdle in the way of privacy protection is the difficulty of foreseeing the side effects associated with fusing information of various sources. This issue manifests typically in information sharing scenarios, particularly those meant for delivering transparency and thus gaining the trust of the public and citizens [39][21][30][31]. Sharing data increases transparency and might lead to an increased chance of privacy breaches. While the former enhances the trust of citizens and individuals in institutions, the latter diminishes the established trust. Sharing data, as a result, becomes a typical wicked problem [38] that requires adopting an elegant design approach that is capable of delivering privacy and transparency by applying appropriate tradeoffs satisfactorily.

Privacy and transparency in the setting of our judiciary data dissemination – in being demand-driven, sustainable, feasible, and research-oriented (see Subsection 2.2) – can be categorized as a typical wicked problem because it satisfies the ten properties of such problems as outlined by Rittel and Webber [33]. We outline these properties in the setting of our judiciary data dissemination in the following.

1. There is no definitive formulation of the problem because "problem understanding and problem resolving are concomitant to each other" [33]. It is impossible to develop an exhaustive inventory of all conceivable solutions ahead of time, for example, in our case to know which information to disseminate, given all possible contexts, laws and user preferences. Constraining the solution space through defining the sub-problems corresponding to our three artifacts has been the essential wicked part of our problem.
2. There is no stopping rule to determine when a solution has been found [33]. Because when the information is released, it is impossible to foresee "the causal chain" [33] that may lead to revealing of some personal information. In our case, we stopped looking for better (or optimum) solutions due to some reasons external to the problem, namely the feasibility constraints (e.g., availability of time and resources).
3. Solutions to the problem are not true-or-false, but good-or-bad, and it is impossible to determine whether a solution is correct based on the examinations of qualified experts independently, according to some firm and formal decision rules to determine the correctness [33]. In our case, see for example the discussion in [27] over the inconsistency of Data Protection Act 1998 and the EU Data Protection Directive 95/46 about when a piece of information can be considered as personal.
4. There is no immediate and no ultimate test of a solution [33]. If one implements a privacy preserving transparency solution within our judiciary setting, she/he should wait enough – "virtually an unbounded period of time – to observe possible waves of consequences and repercussions" [33].
5. Every solution to the problem is a "one-shot operation" because there is no opportunity to learn from mistakes [33]. In our case, the reputation of users, the ministry and the government is severely on stake if the research center comes up with reckless solutions that reveal privacy sensitive information.
6. There is not an enumerable (or an exhaustively describable) set of potential solutions to the problem [33]. This is also the case in our setting, considering the possible information content, operational contexts, user preferences and the laws and legislations. Furthermore, datasets and their labeling can be imperfect, leading to misinterpretations due to such mistakes. Therefore, "it is a matter of judgment which of these solutions should be pursued and implemented" [33].
7. Every information dissemination case is essentially unique as one can find always some properties that distinguish among cases [33]. In our setting, for example, the scope of our data spans over a wide range of personal, social, etc. phenomena; the requesters of our data can have a wide range of expertise, ethical and scientific merits, motivations, data usage objectives, etc.; the context of data access and usage can differ per access; and the laws and regulations are subject to changes. One may attempt to define some classes that are distinctive, but this division and definition in itself is an essential aspect of wickedness [33].
8. The problem of transparency can be considered to be a symptom of another problem, e.g., fear of privacy breaches or lack of trust in authorities. The level at which the problem solver wants to solve the former problem (i.e., transparency) through solving the latter problem (e.g., privacy) "depends on self-confidence of the analyst and cannot be decided on logical grounds" [33]. If the latter problem is not derived/defined well, things can go worse in regard to solving the original problem (i.e., transparency may get compromised drastically).
9. There are numerous ways to explain the existence of a discrepancy that represents the problem [33]. The choice of explanation determines the nature of the problem's resolution [33]. In our setting, for example, some third parties who reuse the released data from our completed research projects might draw invalid conclusions. Such invalid findings might even cast doubt on the results of the official reports of our research projects and can consequently cause, among others, reputational damage for our research center. Having such invalid findings can be explained by lack of metadata documentation or by incompetent/malevolent persons in charge of data interpretation. While the former reason asks for a decision to invest in better metadata documentation, the later reason asks for not sharing the research data.

10. The problem solver has no right to be wrong [33]. One cannot afford realizing an information dissemination solution that endangers privacy of users whose data is supposed to be well guarded by the ministry. Therefore, one should seek a solution that partially "improves some characteristics of the world where people live", instead of trying to find the truth (i.e., to try to find a true and global solution) [33].

As mentioned in [27], there should be nevertheless a non-zero-sum relation between transparency and privacy. This means that successful data disseminations do not necessarily result in violation of privacy and successful privacy protection solutions do not necessarily prevent/obstruct data dissemination. A designer should seek for a mix between transparency and privacy or, as O'Hara [27] formulates it, the designer should "determine the maximum level of transparency consistent with an acceptable level of privacy". One should note that the scope of transparency in our work is wider than that in [27]. While O'Hara [27] considers transparency in regard to releasing reusable data to everyone, with a few restriction, and via accessible infrastructure; our scope includes also releasing sensitive data to individuals and for special purposes (like research, policymaking, education, etc.).

4. DESIGED INTERVENTIONS

In the course of 9 years, starting from 2005, we have designed and operationalized three artifacts to disseminate our data in a privacy preserving way (i.e., to disseminate our judicial information with a mix of transparency and privacy). This section elaborates on how the problem (and solution) space has (have) evolved during the study. Note that here we do not intend to describe all details about the design options and design steps due to space limitations. The objective, nevertheless, is to show how problem redefinition (thus the adopted solutions) has evolved. We first start the section with defining our data types.

4.1 Data types

The research center primarily works with two types of data: Judicial registration data (i.e., raw judicial data that can be extracted from a number of government databases) and judicial research data (i.e., enriched data that the research center or its associates have created in (research) projects). In addition, the research center produces and possesses the so-called statistical information, which can basically be regarded as non-confidential aggregated data. This statistical information is produced based on the judicial registration data and the judicial research data. In summary, the research center's data can be categorized as:

- Judicial registration data,
- Judicial research data, and
- Statistical data.

The research center often removes all privacy sensitive data (attributes) before archiving them. Note that for publicly accessible data, such privacy sensitive attributes are always removed. Data anonymization techniques, for example, are used for this purpose. Typically, statistical information requires minimum amount of or no anonymization. Although data anonymization limits the possibilities of privacy breaches in the future, it also limits reuse of research results or creation of new datasets through linking other data with the disseminated data.

4.2 Design artifacts

We have designed and launched the following three solutions in our research center:

- Restricted access procedure (since year 2005), which has resulted in a procedure for sharing (anonymized) data directly between the research center and data requesters.
- Open access procedure (since years 2008), which has resulted in a procedure for sharing (anonymized) data indirectly between the research center and data requesters, i.e., via a Trusted Third Party (TTP),
- Mashup tool (since 2010), which has resulted in a Web portal for answering specific queries of policymakers of our ministry.

In 2005 we noticed a growing importance of and demand for our data from completed research projects and for our judicial registration datasets. Researchers from universities and (commercial) research institutes, students, policymakers, journalists, civilians were interested in the data. At the time, also the research center was interested in facilitating the reuse of its data to enhance the validity of its data through subjecting it to the public and expert scrutiny. After analyzing the existing infrastructure and practice for data collection and sharing, we found out that the existing laws and regulations provided few guidelines about how to share such privacy sensitive data [37]. Consequently we defined our *restricted access procedure* comprising some guidelines and a structure for authorization of our information sharing. These guidelines stemmed from two basic conditions of preserving privacy and guaranteeing the research center's interests. For example, two privacy related guidelines are: do not share data if the data has any privacy sensitive information and share data if the data release is in compliance with all privacy laws and regulations. As another example, two interest related guidelines are: do not share strategic data that the research center intended to use in the future or have invested a substantial amount of effort in, and share data with the preferred partners. As part of the structure of the authorization procedure, we introduced a central coordinator to receive and manage the data requests, and required the research center's management board to decide over the releases of our raw data (thus not for release of statistical data).

During the operation of the restricted access procedure between 2006 and 2010, we had around 120 data requests each year from end users, where every data request gave us an insight into the boundaries of data sharing with third parties. Around year 2007, there was the open data movement [13] that aimed at making certain data available to everyone and for any use. Furthermore, we experienced some administrative burden for managing the infrastructure, the datasets, and the data requests in the case of the restricted access procedure. Therefore, we desired to somehow reduce the burden by delegating (part of) the data sharing work to the external and trusted parties (and hereby open part of our data to the pubic). Thus, we reformulated the problem to: *how to bring our data to a larger public for (re)use, while preserving privacy and reducing the operational and administrative burden imposed upon the research center*.

We decided to archive some of our datasets at a TTP, from where data requesters could access the archived data directly. In order to make sure that no privacy or misuse issue arises, we crafted a policy document to determine the datasets that can be archived (e.g., by excluding those datasets with privacy risks, anonymizing the archived datasets, defining a list of (privacy) criteria for archiving of datasets). In addition to hosting our data outside the research center, we wanted to distance ourselves as much as possible from the 'restricted access' model and to move towards an opener data release model. We therefore made our archived data accessible to all data requesters (i.e., the public) and for any

use initially. These processes of data archiving at and data access from the TTP formed our *open access procedure*. Within the period of 2007-2010 there were only 3 datasets from our 207 datasets anonymized and then archived. Apparently the project managers in charge of project datasets were unwilling to open up their datasets prevalently. Note that the unit of analysis for the open access procedure is the number of datasets archived at the TTP, while the unit of analysis for the restricted access procedure is the number of data requests by end-users.

In the period of 2010-2011, we carried out a legal study that concluded that privacy laws and regulations principle allow the research center to reuse the data for its scientific research and share the data with third parties for scientific research. In another research we also found out that although anonymized or aggregated data may not seem personal data at first glance, it may become personal data by combining it with other publicly available data. Consequently we limited the target group who may receive our research data in both open access and restricted access procedures to the *scientific researchers* who want to use our data only for *scientific research purposes* (i.e., for universities and governmental research centers). From a privacy protection viewpoint we found data release can be acceptable for this target group because scientists are less susceptible to data misuse, misinterpretation and privacy breaches (due to their strict code of conduct). Furthermore, scientists usually publish their results in peer-reviewed papers. Publication of scientific papers can be regarded as providing an *implicit* feedback from data requesters to our research center on how responsibly the center's data is treated and used. Moreover, in the case of the open access procedure we devised a number of closed questions to help dataset controllers to identify and rule out release of sensitive datasets via the open access procedure (and consider releasing them via the restricted access procedure). For the open access procedure, nevertheless, we found that the project managers in control of our research data were still unwilling to give permission to upload their datasets to the TTP, even after we restricted the release of those datasets only to researchers and for scientific research, and after we devised the new decision making process for archiving our data. Specifically there were 9 out of our total 207 datasets archived at the end of this period (previously it was 3 out of 207 datasets).

Next to limiting the usage scope to scientific purposes, having the implicit feedback were considered instrumental by the practitioners of the research center for data archiving in the open access procedure. Therefore, we reformulated the problem around year 2012 to: *how the amount of feedback can be increased in the case of the open access procedure*. Based on a literature study, we found out that having explicit feedback about the usage of the archived data at the TTP can convince our data controllers and augment their trust in order to share their data [16] [35]. We decided therefore to embed an explicit feedback in the procedure to allow the research center to negotiate with data requesters directly before granting them access to the data and hereby to check their adherence to privacy laws and regulations (e.g., finality, legitimacy, proportionality, subsidiarity, transparency, and data subjects' rights). The necessity of receiving such feedback stems from the fact that the data controller (i.e., our research center) is morally, ethically and legally responsible for any breach, misuse, etc. of the disseminated data [4]. In discussions within the research center also another bottleneck was identified, namely: who has the final responsibility of data release. To address this problem, we decided to reintroduce part of the restricted access procedure by adding the decision of the board of department heads for granting access to data requesters. Hereby the scope of feedback is extended to the center's department heads. We also reintroduced a standard contract to be signed by data requesters before granting the access. Following all amendments of the redesign of the open access procedure, we were able to convince project leaders to archive 15 extra datasets of our completed quantitative research projects. Now, we have a total of 24 archived datasets at the TTP. This number of 24 projects amounts to 24/207 = 12% of the total quantitative research projects that are archived at the research center. Finally, we learnt from the practice that feedback could be important not only for preserving privacy but also for combating possible data misinterpretation and misuse [4]. At this stage of our study we also gained strategic understanding about the reasons behind not archiving the remaining datasets at the TTP (because the remaining datasets are confidential, acquired from third judicial parties under the strict condition to be used for a specific research project or to be reused by the research institute itself on relatively short term). Thus our study provided us with a realistic view on the potential of opening our datasets.

In 2009 we perceived that policymakers within the ministry (have) had a practical need for statistical insights into public safety at different geographical levels of a society, ranging from national to regional level. The policymakers could use such insights to shape effective and sound policies. For example, if it appears that some parts of the country are becoming less safe compared to the other parts of the country, policymakers may decide to spend more resources in the deteriorating parts than in the stable parts of the country. This need of policymakers reshaped our problem of data sharing to: *How to share our data with the policymakers within the ministry in a privacy preserving and automatized way* as these colleagues had no database and data management skills. Consequently, we developed a mashups tool based on Web 2.0 technology to dynamically collect raw data from various datasets of the Dutch Ministry of Security and Justice and to disseminate the enriched data to the policymakers within the ministry [9]. A policymaker, as the end-user of the tool, could pose a query and the mashups tool provides a reply with the answer to the query and some contextual information. Such an information-sharing tool, therefore, can be characterized as a software tool of the restricted data access model that delivers data on demand, to a set of specific queries, in an automatic way, and for the policymakers within the ministry.

In order to preserve privacy, the Web presentation layer of the mashups tool performs some checks to minimize privacy violations before presenting the query outputs. Regardless of the security preserving features implemented in data collection and distribution processes, some inquiry results might reveal personally identifiable information, which could result in privacy breaches. To address this problem we built a control mechanism at the Web presentation layer to check privacy violation risks for the information to be revealed. This check is rule-based and is carried out automatically. Should there be a chance of revealing privacy sensitive information, the presentation layer stopped or limited the information to be displayed. This last stage control can be considered as an internal feedback loop within the system that allows the mashups presentation layer to inform the mashups' internal components when privacy requirements are not met at the presentation stage. This feedback stops the internal components disseminating any further information.

5. DISCUSSION

In this section we first summarize the main results achieved through our designerly work outlined in Section 4. Subsequently,

we discuss our contributions according to the criteria mentioned in [38].

5.1 Achieved results

Our research center's strategy that is based on the feasibility, sustainability, demand-driven, research oriented principles has resulted in three (procedural) artifacts to disseminate judicial data (i.e., to deliver governmental transparency) in a privacy preserving way. Here we provide a snapshot of the results achieved since 2005 through these three artifacts based on the three criteria of the data recipient scope, the detail level of the disseminated data, and the ease of the data dissemination/access processes. Figure 2 provides a schematic comparison among these artifacts according to these criteria whose choice is inspired by the work of O'Hara [27]. O'Hara considers transparency as releasing reusable data (i.e., related to the level of data details criterion) to everyone (i.e., related to the scope of data recipients criterion) with a few restrictions and via an accessible infrastructure (i.e., related to the ease of data access criterion). Note that our notion of transparency is wider than O'Hara's as ours includes also releasing sensitive data to individuals, for specific purposes (like research, policy making, education, etc.) and within specific organizations (like within our ministry).

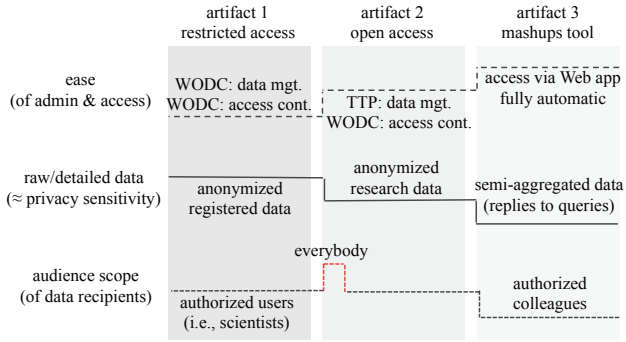

Figure 2. A comparison of the three artifacts developed.

The scope of data recipients ranges from the public (i.e., data being open to everyone) to the specific (i.e., individuals within an organization). As illustrated in Figure 2, the data is made transparent for authorized users in all three artifacts, while the third artifact took a more restrictive turn and offered the data only to the users within our ministry. Also shown in the figure is our attempt to open our data to the public in the beginning stage of the second artifact's development but it turned out to be infeasible subsequently. The level of details in disseminated data, which can be related to privacy sensitivity, can range from raw data (i.e., judiciary registration data), to processed data (i.e., judiciary research data), and highly aggregated data (i.e., statistical data). Figure 2 shows in the middle that the detail level of the revealed data drops in the third artifact relatively because the mashups tool plays a mediator role and translates raw data in our datasets to high-level responses for the specific queries of policymakers. The ease of data access for data recipients (or the workload of data disseminators) ranges from data management and access control directly at our research center, at the TTP, or in an automatic way (i.e., via a web application). As the figure shows this aspect is incrementally improved from artifact one to artifact two (the data is managed outside our organization but the access control is done via the research center); and from artifact two to artifact three (data access is fully automated, given the set of the queries possible).

Note that the comparison above does not encompass the highly aggregated judiciary data (i.e., our statistical information) because it is made open for everyone through the Internet since the beginning due to absence of any privacy sensitive information. Also a quick glance at the comparison in Figure 2 reveals that our efforts to open our judiciary registration and research data (the raw or slightly processed data) to a larger public were unsuccessful in the course of these years and despite our continuous efforts. The ease of access to and administration burden of data, however, have been improved due to these efforts.

Our research demonstrates that, after processing of disseminated information, it is useful to enable data disseminators (i.e., the data controllers who act on behalf of data subjects) to know about (some aspects of) the data usage. In information sharing settings this can be realized by providing a feedback from information processors (like the end-users or computer systems who receive the disseminated information) to the data disseminators when, for example, the data is actually used or privacy sensitive data is revealed due to processing of the shared data. The improved ease of information dissemination for artifact 2 compared to artifact 1 in Figure 2 can be attributed to embedding the feedback mechanism in the open access procedure (i.e., artifact 2).

5.2 On research contributions

In order to distinguish the contributions of a designerly work as research and not as normal works of practice, Zimmerman et al. [38] proposed two ways to differentiate among design research artifacts from design practice artifacts[1], namely: having the research intent of producing knowledge (not just to make a commercially viable product) and producing innovative contributions (not just refinements of existing products). The research intent is explained in Subsection 5.2.1. Research contributions of such an endeavor can be shown through describing the process, invention, relevance, and extensibility aspects of the work carried out [38]. We have already described the design and development processes of our artifacts in Section 4 (although at a high level due to space limitations). Therefore, we describe in the following only the innovative aspects (Subsection 5.2.2), and the relevance and extensibility aspects (Subsection 5.2.3).

5.2.1 Intent

As underlined in Subsection 2.2, one of the key characteristics of our strategy is to carry out a sustainable research agenda through acquiring and producing new knowledge for identifying and/or solving (new) problems relevant for our ministry. This new knowledge acquisition/production is a key effort to increase our center's viability among the stakeholders within and outside the ministry. As a testimony to this claim, there have already been a substantial number of publications of the research center on the topic in scientific conferences and journals, for example see [4][7][8][9][10][11][18][23][39] and [40].

5.2.2 Innovation

On preserving privacy while disseminating judiciary data: There are various (open data) initiatives to release public sector data to citizens as a means of government transparency. Such initiatives provide citizens with an insight in governmental agencies as well as deliver added value services through integration of the released

[1] Note that these criteria are for a research through design methodology, which is similar to the designary approach adopted in our study.

public data with other data. An example of such a transparency initiative in the area of judiciary data is the Website [32] that publishes various information items about, among others, court verdicts within the Dutch Judiciary and the Supreme Court. The site uses the suppression method for anonymization by removing the names, birthplaces and exact birthdates of suspects, witnesses and victims. Other information about the investigation, prosecution and court procedures is openly communicated and published. The website does not intend to provide a bulletproof data anonymization process because, in our opinion, it is concerned with providing aggregated court data (it is possible to derive some of the removed information by using a simple Google search [3]). Similarly, we were able to openly publish the highly aggregated statistical information of our research center (with applying minor data anonymization if it was necessary). Opening other data types of our research center (i.e., judicial registration data and judicial research data) was not possible in the generic sense that O'Hara [27] defines the term transparency as "… release of datasets not to individuals, but to everyone, in reusable form, with few restrictions of use (e.g. under the Open Government License), via an accessible infrastructure (such as the World Wide Web) …". Our experience has shown that preserving privacy with this level of transparency seems too ambitious for our datasets, considering the legal and ethical considerations. Therefore, we had to reduce the level of transparency by downsizing the scope of data release (i.e., audience, detail level, or the data transfer medium as reflected upon in Subsection 5.1).

On wicked problems and privacy: The problem of information transparency (and subsequently creating a mix between privacy protection and transparency) is positioned as a wicked problem in this contribution. The term mix here should not be considered as a metaphor for finding a balance point or a fulcrum point at which a 'correct' amount of privacy and transparency can be achieved. For another wicked problem (i.e., the security and privacy problem in policy making settings), Taipale [34] does not prescribe using the term balance in the sense of the fulcrum point mentioned. This is because wicked problems generally have infinite potential outcomes, due to interest diversity of the stakeholders involved and the social context in which they take place. Our search for a mix between transparency and privacy, in essence, was not focused on finding the correct balance point, but was aimed at finding a realistic point, given the existing constraints (specially those pertained to our research center's strategy). Hereto we did manage to realize and intervene three artifacts that helped our research center to attain a preferred state in terms of disseminating its judicial data in a privacy preserving way. Similar to our formalization of the privacy problem, Ackerman [1] regards the attempts that aim at dealing with online privacy nicely as a wicked problem "in the computer science sense of wicked, meaning an ill-formed, intractable problem", see also [15]. So far, however, we have not found any work that describes finding a practical solution for the privacy problem as a sort of wicked problems (specially in judicial data release settings).

On feedback: Providing feedback from data processors to data controllers/subjects can enhance trust of the latter group in the data dissemination process [4], encouraging them to share data. Tsai et al. [35] investigate the effect of feedback on sharing location information with requesters of such information. They show that those users who had access to the logs of their location information requests reported greater comfort levels in using the system and a reduced privacy concerns, compared to those who received no feedback of their location information requests. As another example, the Buddy Tracker application [16] feeds back location information requests to the users in real time and the authors claim that providing such feedbacks contributes to social translucency of users, whereby users use group-based systems more efficiently. Similarly, feedback as a trust enhancement mechanism (through enforcing accountability) is also considered in cloud computing [19][20][28]. The feedback mechanisms proposed in these works are used to generate reports and summaries of, for example, audit trails, file access history, file lifecycle and suspected irregularities to end users.

There is also a body of work that proposes using feedback to inform the data subjects/controllers, about their information being requested by others, before granting the access, see for example [22][24][25]. These feedbacks are often of type 'consent' management in the context of data usage to allow data subjects/ controllers to consent or dissent to their personal data passing across entities. Our implementation of explicit feedback in the case of the open access procedure is similar to the implementations mentioned in [22][25] for sharing user-context and user-identity attributes with third parties, respectively. In all these the feedback is used to ask for consent and/or to further specify the data access and privacy policies per data sharing instances. While the feedback mechanisms presented in [22][25] are of technical nature, our feedback solution encompasses both technical and procedural aspects and, as such, offers a cross-organizational solution for preserving privacy. Our solution is applicable across organizations because the organizations involved can negotiate terms of use and access at a procedural level using also traditional means like postal correspondences, telephone calls and face-to-face meetings. This compatibility with traditional mechanisms, therefore, makes the solution suitable for cross-organizational settings where processes are not (or cannot be) fully automated.

5.2.3 Relevance and extensibility

In addition to being research-oriented and having innovative aspects, our artifacts have been operationalized in a real world setting (i.e., within our research center, with real judiciary data, by real users). The incremental and extensible aspect of the work enabled us to built upon previous results and feed current outcomes to future developments. The restricted access procedure is now operational for almost 9 years, and has faced a few minor revisions since its early development stages. The open access procedure has faced some challenges in its development. In archiving the anonymized datasets to the TTP we faced resistance of project managers (i.e., the data controllers) against uploading. Improving the open access procedure in a few steps mentioned enabled us to convince project leaders and the heads of departments to archive their data at the TTP (an eight folds increase, from 3 to 24 datasets). The mashups tool, in turn, has been in use by policymakers to answer their queries and questions.

Within and across the three developed artifacts, we were able to reuse the gained knowledge in subsequent stages. For example, the insight on feedback infused from the open access procedure to the mashups tool, the opening of our judiciary data for scientists and for scientific purposes inspired both restricted and open access procedures, and the experience gained from developing one artifact is used to influence the design and intervention of the following artifacts.

6. CONCLUSIONS

Adopting a designerly approach, we have realized three information dissemination artifacts within our research center,

which are still operational currently. In designing and building these artifacts we aimed at addressing the wicked problem of transparency (i.e., information sharing) by trying to preserve privacy sensitive information. As these artifacts were designed/realized almost sequentially, we adapted the problem scope (and solutions accordingly) based on the lessons learnt from each artifact's realization and based on the arising issues and conditions during the study. One can summarize the gradual redefinitions of the problems as follows: How to facilitate the reuse and to enhance the validity of our data through subjecting it to experts scrutiny; how to bring our data to a larger public for reuse in a way that the operational and administrative burdens remain acceptable; how to enhance the trust of data controllers so that they share their data willingly, and how to share our data in a fully automatized way. During all these readjustments, we considered addressing the problem of privacy as the instrument to address the transparency problem.

Providing feedback to information disseminators about privacy concerns – thus, in practice, putting the information disseminators in the control loop of these privacy concerns – rose as an effective means to facilitate information dissemination. The open access procedure showed how having such explicit and implicit feedbacks (i.e., redirecting data requests to our research center by TTPs and having the peer review process of scientific papers) encouraged our project managers to share their information with scientific community. In this way, it became possible to eliminate or to reduce the (self-imposed) resistance against dissemination of information. It is for our future research to investigate other efficient feedback mechanisms, especially when information travels multiple hops away from the original disseminator. Furthermore, the context of information use and processing is a determinant factor to base the decision of privacy sensitive information release on, as we have learnt during development of the restricted access and open access procedures.

7. REFERENCES

[1] Ackerman M.S. 2001. The intellectual challenge of CSCW: the gap between social requirements and technical feasibility. In: Carroll JM (ed) *Human–Computer Interaction in the New Millennium.* Addison-Wesley, New York.

[2] Bargh, M.S., Choenni, R., Mulder, I. and Pastoor, R. 2012. Exploring a warrior paradigm to design out cybercrime. *In Proceedings of Intelligence and Security Informatics Conference (EISIC'12)*, Odense, Denmark, Aug. 22-24, pp. 84-90.

[3] Bargh, M.S. and Choenni, S. 2013. On preserving privacy whilst integrating data in connected information systems. *In Proceedings of the International Conference on Cloud Security Management (ICCSM'13)*, Seattle, US, 17-18 October.

[4] Bargh, M.S., Choenni, S., Meijer, R. and Conradie, P. 2014. Privacy protection in data sharing: towards feedback based solutions. *In Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance (ICEGOV)*, Guimarães, Portugal, 27-30 October.

[5] Bertot, J.C., Jaeger, P.T., and Grimes, J.M. 2012. Promoting transparency and accountability through ICTs, social media, and collaborative e-government. *Transforming Government: People, Process and Policy,* vol. 6, nr. 1, p.p. 78-91.

[6] Boyd, D. 2010. Privacy and publicity in the context of big data. *Opening Keynote at the WWW'10 Conference*, Raleigh, North Carolina, Online, Available: http://www.danah.org/papers/talks/2010/WWW2010.html [retrieved on Oct. 28, 2012].

[7] Braak, S. 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 (DG.0'12)*, Jun. 4–7, College Park, MD, USA, pp. 135-144.

[8] Choenni, R., Dijk, J. van and Leeuw, F. 2010. Preserving privacy whilst integrating data: applied to criminal justice. *In Information Polity - an International Journal of Government and Democracy in the Information Age*, vol. 15, nr. 1-2, pp. 125-138.

[9] Choenni, R. and Leertouwer, E. 2010. Public safety mashups to support policy makers. *In Proceedings of International Conference of Electronic Government and the Information Systems Perspective (EGOVIS'10),* Bilbao, Spain, Aug. 30-Sept. 3, pp. 234-248.

[10] Choenni, R., Waart, P. van and Haan G. de 2011. Embedding human values into information system engineering methodologies. *In Proceedings of ECIME'11*, Como, Italy, Sep. 8-9.

[11] Choenni, S., Bargh, M.S., Roepan C. and Meijer, R. 2014. Privacy and security in data collection by citizens. Book chapter in *Smarter as the New Urban Agenda: a Comprehensive View of the 21st Century City*, edited by J.R. Gil-Garcia, T.A. Pardo and T. Nam, Springer LNCS, (in press).

[12] Conger, S. and Landry, B.J.L. 2008. The intersection of privacy and security. *Sprouts: Working Papers on Information Systems*, vol. 8, nr. 38.

[13] Conradie, P. and Choenni, S. 2012. Exploring process barriers to public sector information release in local government. *In Proceedings of 6th Int. Conf. on Theory and Practice of Electronic Government (ICEGOV'12)*, Albany, USA, Oct. 22-25, ACM Press, USA, pp. 5-13.

[14] Cross, N. 2001. Designerly ways of knowing: design discipline versus design science. *Design Issues*, vol. 17, nr. 3, pp. 49–55.

[15] Dwyer, C. 2007. The inference problem and pervasive computing. *Proceedings of Internet Research 10*.

[16] Jedrzejczyk, L., Price, B.A., Bandara, A.K. and Nuseibeh, B. 2010. On the impact of real-time feedback on users' behavior in mobile location-sharing applications. *In Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS)*, ACM Press, New York, pp. 1.

[17] Kagal, L. and Abelson, H. 2010. Access control is an inadequate framework for privacy protection. *W3C Privacy Workshop*, June 1–6. Retrieved from http://202.154.59.182/ejournal/files/Access control is an inadequate framework for privacy protection.pdf

[18] Kalidien, S., Choenni, S. and Meijer, R. 2010. Crime statistics on line: potentials and challenges. *In Proceedings of the 11th International Conference on Digital Government Research (DG.O)*, Puebla, Mexico, May 18-21, ACM Press, New York.

[19] Ko, R. K., Lee, B. S. and Pearson, S. 2011. Towards achieving accountability, auditability and trust in cloud

computing. *In Advances in Computing and Communications*, Springer, pp. 432-444.

[20] Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q. and Lee, B. S. 2011. TrustCloud: a framework for accountability and trust in cloud computing. *In Proceedings of World Congress on Services (SERVICES)*, IEEE Press, pp. 584-588.

[21] Kulk, S. and van Loenen, B. 2012. Brave new open data world? *In International Journal of Spatial Data Infrastructures Research*, vol. 7.

[22] Laube, A. and Hauser, S. 2013. myIdP - the personal attribute hub. *In Proceedings of the 5th International Conferences on Advanced Service Computing (SERVICE COMPUTATION).*

[23] Meijer, R., Choenni, S., Sheikh Alibaks R. and Conradie, P. 2013. Bridging the contradictions of open data. *In Proceedings of the 13th European Conference on e-Government*, Varese, Italy 13-14 Jun. 2013, pp. 329-336.

[24] Mont, M. C., Pearson, S., Kounga, G., Shen, Y. and Bramhall, P. 2009. On the management of consent and revocation in enterprises: setting the context. *Technical Report HPL-2009-49*, HP Labs, Bristol.

[25] Mont, M. C., Pearson, S., Creese, S., Goldsmith, M. and Papanikolaou, N. 2011. A conceptual model for privacy policies with consent and revocation requirements. In Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R. and Zhang, G. (Eds.), *IFIP Advances in Information and Communication Technology*, V. 352, Springer, pp. 258–270.

[26] Nissenbaum, H. 2004. Privacy as contextual integrity. Washington Law Review, 79(1), pp. 101–158.

[27] O'Hara, K. 2011. *Transparent Government, not Transparent Citizens: a Report on Privacy and Transparency for the Cabinet Office*. Technical Report, Retrieved from http://eprints.soton.ac.uk/272769/

[28] Pearson, S. and Charlesworth, A. 2009. Accountability as a way forward for privacy protection in the cloud. *In Cloud Computing*, Springer, pp. 131-144.

[29] Pittenger, D. J. 2003. Internet research: An opportunity to revisit classic ethical problems in behavioral research. *Ethics and Behavior*, vol. 13, nr. 1, pp. 45-60.

[30] Raad voor het Openbaar Bestuur (ROB) 2012. Gij zult openbaar maken; Naar een volwassen omgang met overheidsinformatie (in Dutch). Sept., ISBN 978-90-5991-068-3.

[31] Rajamäki, J., Tervahartiala, J., S.Tervola, Johansson, S., Ovaska, L. and Rathod, P. 2012. How transparency improves the control of law enforcement authorities' activities? *In Proceedings of European Intelligence and Security Informatics Conference EISIC'12*; Aug. 22-24, Odense, Denmark, pp. 14-21.

[32] Rechtspraak 2013. *Website of the Dutch Judiciary and the Supreme Court of the Netherlands*, [Online], http://zoeken.rechtspraak.nl/default.aspx.

[33] Rittel, H. and Webber, M. 1973. Dilemmas in a general theory of planning. *Policy Sciences*, 4, December 1969, pp. 155–169. Retrieved from http://link.springer.com/article/10.1007/BF01405730

[34] Taipale, K.A. 2004. Technology, security and privacy: The fear of Frankenstein, the mythology of privacy and the lessons of King Ludd." *Yale JL and Tech*. 7: 222.

[35] Tsai, J. Y., Kelley, P., Drielsma, P., Cranor, L. F., Hong, J. and Sadeh, N. 2009. Who's viewed you? The impact of feedback in a mobile location-sharing application. *In Proceedings of Computer Human Interaction (CHI)*, ACM Press.

[36] Tschantz, M.C. and Wing, J.M. 2009. Formal methods for privacy. *In Proceedings of the 2nd World Congress on Formal Methods*, pp. 1-15.

[37] Winter, H.B., de Jong, P.O., Sibma, A., Visser, F.W., Herweijer, M. Klingenberg, A.M. and Prakken, H. 2008. Wat Niet Weet, *Wat Niet Deert; Een Evaluatieonderzoek Naar de Werking van de Wet Bescherming Persoonsgegevens in de Praktijk.* Technical Report at WODC (in Dutch*)*, Den Haag.

[38] Zimmerman, J., Forlizzi, J. and Evenson, S., 2007. Research through design as a method for interaction design research in HCI. *In Proceedings of CHI 2007, Design Theory*, Apr. 28-May 3, San Jose, CA, USA.

[39] Zuiderwijk, A., Janssen, M., Meijer, R., Choenni, R., Charalabidis, Y. and Jeffery, K. 2012. Issues and guiding principles for ppening governmental judicial research data. In: H.J. Scholl et al. (Eds.): *EGOV 2012*, LNCS 7443, pp. 90–101.

[40] Zuiderwijk, A., Janssen, M., Choenni S. and Meijer, R. 2014. Design principles for improving the process of publishing open data. *Transforming Government: People, Process and Policy*, vol. 8, nr. 2.