Unlocking the Value of Public Sector Personal Information Through Coproduction

Walter Castelnovo

Abstract In their day-to-day operations, public sector organizations collect and use huge amounts of information that if made available for re-use would contribute to economic growth. Much of this information directly or indirectly can lead to the identification of 'natural persons' and, as such, the personal data protection regulation applies to it. According to the General Data Protection Regulation (GDPR) issued by the EU in 2016, unless it is regulated by a specific legislation, personal information can be processed only based on the data subject's explicit consent. This raises the question of what strategies public organizations could implement to make the data subjects willing to allow the (possible) re-use of their personal information. By elaborating on evidences from the economics and the psychology of privacy literature, the paper suggests that public sector organizations can implement a coproduction strategy to unlock the value of public sector personal information in a user-centric personal information ecosystem. More specifically, the paper argues that the data subjects can be made more willing to consent to the processing (and possibly to the re-use) of personal information by involving them as coproducers in the processes through which public sector organizations can support economic growth in the digital society.

Keywords Coproduction · Public sector information · Privacy · Personal information

1 Introduction

Information is the fundamental resource in the Digital Society. The pervasive diffusion of devices with high information processing capacity and low cost allows producing huge amounts of information every day. People using personal information processing devices produce an ever-increasing share of this information. Spieker-

W. Castelnovo (✉)
University of Insubria, Varese, Italy
e-mail: walter.castelnovo@uninsubria.it

A. Lazazzara et al. (eds.), *Exploring Digital Ecosystems*,
Lecture Notes in Information Systems and Organisation 33,
https://doi.org/10.1007/978-3-030-23665-6_27

mann et al. [47] report that every day individuals send or receive 196 billion e-mails, submit over 500 million tweets and share 4.75 billion pieces of content on Facebook. This information is generated by individuals and (directly or indirectly) pertains to individuals; hence, it should be considered as personal information, according to the extended definition of Kang [22].

Acquisti et al. [2, p. 444] observe that "individuals' traits and attributes (such as a person's age, address, gender, income, preferences, and reservation prices—but also her clickthroughs, comments posted online, photos uploaded to social media, and so forth) are increasingly regarded as business assets that can be used to target services or offers, to provide relevant advertising, or to be traded with other parties". This explains why personal information is increasingly being considered as a fundamental economic asset, the new 'oil' of the 21st century [53], an important currency in the new millennium to which also a relevant monetary value can be associated [51].

While a remarkable value resides in personal information, it often remains untapped due to the quite stringent limitations the privacy preserving regulations impose on its use by both public and private subjects. According to the World Economic Forum, creating a user-centric personal information ecosystem in which "individuals can have greater control over their personal data, digital identity and online privacy" and where individuals "would be better compensated for providing others with access to their personal data" [53, p. 10], can represent a possible strategy for unlocking the value of personal information. If the control (if not legal ownership) over personal information is given back to them, the data subjects are allowed "to decide whether and with whom to share their personal information, for what purposes, for how long, and to keep track of them and decide to take them back when so wished" [16, p. 5].

This raises the research question the paper intends to address, i.e. what strategies can organizations implement to make the data subjects willing to share their personal information, once the control over that information is given back to them? This is a timely endeavor, since new regulations are being issued that grant to the data subjects more control over the use of their data. An example of such regulations is the General Data Protection Regulation (GDPR) issued by the European Parliament in 2016 that represents an important step toward the establisment of a user-centric personal information ecosystem [43].

The GDPR defines stricter obligations for the data controller (defined as the natural or legal person, public authority, agency or other body which determines the purposes and means of the processing of personal data) to ask for explicit consent to process personal information. Moreover, the new regulation establishes some new rights for the data-subjects: the right to obtain from the data controller access to and rectification or erasure of personal information; the right to restrict or object to the processing of personal information; and the right to data portability.

The GDPR provisions reinforce the data subjects' control over the processing of personal information, defined as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. This could limit the possibility of re-using per-

sonal information since according to the GDPR, unless a specific regulation applies to it, personal information can be processed only based on the data subjects' explicit consent (Article 6.1.a).

This qualitative paper, which is based on a conceptual research approach [31], tries to answer the research question above by considering the case of personal information collected and used by public sector organizations (PSOs) without being mandatory for the data subjects to provide them (for instance, information collected from sensor networks in smart cities). The case of the processing of personal information collected by public sector organizations is interesting since, different from non-public organizations, PSOs can offer the data subjects neither economic compensation nor non-monetary benefits specifically delivered to them in order to obtain the consent to process their personal information. However, evidences from the economics and psychology of privacy literature suggest that economic compensation is not the only reason that could motivate data subjects to disclose their personal information. Empirical researches found that psychological elements related to self-expression, self-efficacy and self-identity provide a better explanation of the individuals' online disclosure behaviors than motivations related to economic compensation or non-monetary benefits.

Interestingly, in the marketing literature these elements have been related to the benefits (potentially) deriving from the coproduction experience. Based on this observation, the paper suggests that PSOs could implement a coproduction strategy to unlock the value of public sector personal information (PSPI) in a user-centric personal information ecosystem. More specifically, the paper argues that, by assuming a concept of privacy as data control [6, 56], the data subjects' consent to allow PSOs to collect, use and (possibly) make available for re-use information pertaining to them can be considered as the individuals' contribution to the processes through which PSOs can support economic growth in the digital society. Such contribution amounts to the individuals' provision of a critical resource, which is what the coproduction of public services usually amounts to.

2 The Impact of the Data Protection Legislation on the Re-use of Public Sector Personal Information

The technological evolution makes available to individuals and to public and private organizations devices, tools and services that allow generating every day huge amounts of information. According to IDC's 2017 Digital Universe update, the number of connected devices is projected to expand to 30 billion by 2020 and to 80 billion by 2025 when the amount of data created and copied annually will reach 180 Zettabytes (180 trillion gigabytes). The dimension of the phenomenon supports the emerging of a new data-driven economy whose value in the EU was €285 billion in 2015 and that is expected to increase to €739 billion by 2020 if favorable policy and legislative conditions are put in place in time and investments in ICT are encouraged.

Fostering Open Data policies is among the strategic actions that could have high impact on the development of the EU data-driven economy. The implementation of the open data policies directly involves public sector organizations since the public sector is one of the most data-intensive sectors. In their day-to-day operations, PSOs process large amounts of information (including demographic, socio-economic, geographical, meteorological and municipal management data, as well as data from publicly funded research projects and digitized books from libraries) that if shared could be of great value for both people and firms. According to an EU Commission report, the total direct economic value of public sector information (PSI) is expected to increase from a baseline of €52 billion in 2018 for the EU28, to €194 billion in 2030, whereas the indirect economic value is estimated to be between 3.5 and 3.78 times as large as the direct economic value [1]. Due to this value of public sector information, many governments worldwide implemented policies to foster PSI re-use, also as open data, as a way to contribute to economic growth in the digital society. This is the principle at the basis of the EU Directive on the re-use of PSI, currently under revision, and the open data/open government policies implemented by many EU national governments [21, 37, 58].

Much of the public sector information contains personal information, both 'ordinary' and sensitive [41, 44], that can be qualified as public sector personal information (PSPI). To PSPI the data protection legislation applies, which could limit severely the possibility of re-using PSPI to contribute to value creation in the data-driven economy. This could be a problem since personal information is among the most valued information for companies operating in the sector. Liem and Petropoulos [26] estimate that applications built on personal information can provide quantifiable benefits of as much as €1 trillion annually by 2020, with a benefit of about € 330 billion annually accruing to private and public organizations. For this reason, besides policies to foster open data, also measures concerning personal data protection and consumer protection are among the strategic actions that are expected to have high impact on the development of the EU data-driven economy.

The General Data Protection Regulation (GDPR), issued by the European Parliament in 2016, is one such measure. By defining reinforced rules on use and consent, on profiling and on the obligations of companies when handling personal information, the GDPR is expected to reinforce trust of citizens resulting in a continuous sharing of personal information as an important input for value-added data services. Moreover, rules on consent of re-use of data for purposes different from the original purpose of collection, and data minimization will allow Big Data analytics to exploit more data with fewer restrictions.

The GDPR gives a quite extensive definition of personal information as any information relating to an identified or identifiable natural person. This definition of personal information as personally identifiable information is strictly related to the idea of privacy as 'the right to be let alone', as defined by Warren and Brandeis in 1890 [22, 45]. Based on this concept of privacy, the processing of personal information must be limited because it can lead to the identification of an individual, which could represent an intrusion in his private life.

Influential as it has been, the definition of personal information as personally identifiable information appears to be problematic in the highly interconnected world of today in which individuals are embedded in complex networks of relationships that make the distinction between the public sphere and the private sphere more and more blurred. Moreover, the technological evolution, the increasing amount of publicly available information, the diffusion of data analytics tools and the emergence of powerful re-identification algorithms have made the personally identifiable information concept critical since even anonymized data could have significant privacy consequences [39, 50]. This impacts also on open data initiatives: open data that do not seem to be personal data on first glance may become personal data by combining it with other publicly available information or when it is de-anonymized [24].

There are already plenty of examples of publicly available information released as open data that have been used to identify individuals [19, 20, 40, 49]. Aggregated or anonymized information contained in open data set that do not allow the identification of individuals when released, may become personally identifiable information as more and more powerful re-identification tools and auxiliary information become available [15].

The GDPR tries to avoid, or at least to reduce, these risks for privacy by assuming an extensive definition of 'identifiable':

> To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. (Recital 26)

According to this definition, the concept of personal information should be considered as a dynamic concept since with the development of technology more and more information can fall under the characteristics of personal information and, consequently, should be treated according to the privacy protection rules [57]. This can determine critical consequences on the possibility to exploit the value of PSPI (and, more generally, of personal information) to create value within the emerging data-driven economy. In fact, any information that in the future might be linked to individuals, should be considered and treated *today* as personal information [24, 28]. Moreover, if information shared today as open data becomes personal information in the future simply because technological developments have made it possible to use it to identify individuals, how can privacy breaches be avoided, given that it is very difficult to effectively remove information once it has been published? According to the GDPR (article 6), in order to be lawful the processing of personal information must be based on the data subject's consent (as a general rule). How can the data subject's consent be obtained for the processing of information that has been published (possibly) a long time before?

If PSI containing personal information is made available for re-use, the application of the principles of data protection stated in the GDPR will create a tension, if not a contradiction, between two apparently conflicting principles. On the one

hand, the need to contribute to economic growth through the sharing of PSPI, which can potentially lead to the (re)identification of individuals. On the other hand, the need to safeguard the individuals' privacy that, in the EU legislation, is considered a fundamental human right [20, 38]. This makes the re-use of PSPI a non-trivial matter, which makes the simplest choice to exclude as much PSI containing personal information as possible from the scope of PSI legislation [1, p. 137] thus leaving an huge amount of potential value untapped [21, 28, 59].

3 Privacy and Personal Information Protection in an Interconnected and Networked World

The notion of data protection originates from the individuals' right to privacy: how privacy is conceptualized influences the definition of personal information and, consequently, the scope of the data protection legislation as well. Depending on how extensive the definition of personal information is, the possibility of processing certain classes of information pertaining to individuals is limited or even excluded.

As observed by Erich Andersen, Deputy General Counsel of Microsoft's Windows Division, "in the digital era, privacy is no longer about being 'let alone'. Privacy is about knowing what data is being collected and what is happening to it, having choices about how it is collected and used, and being confident that it is secure" [7]. Westin [56, p. 7] defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". Hence, privacy can also be defined in terms of the "control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability" [30, p. 10]. Based on this definition of privacy, an alternative definition of personal information emerges as "the information over which a person has some interest or control, in order to negotiate their environment or order their lives" [23, p. 8].

Although the data-control view of privacy is not immune of problems [6, 46], it makes obsolete the traditional distinction between personally identifiable and non-personally identifiable information that, as observed above, is blurring in the digital world of today. Moreover, it shifts the focus of the protection of privacy to the user-based understanding of the perceived risks associated with different types of personal information [32]. Giving individuals the control over the management of the information pertaining to them entails a shift from the traditional organization-centric personal information ecosystem to a user-centric personal information ecosystem. In the organization-centric ecosystem, the management of privacy is delegated to the organizations that process personal information. By agreeing on the terms and conditions defined by the data collectors, individuals delegate to them the protection of their data. On the contrary, in the emerging user-centric ecosystem, the data subjects are allowed to decide whether and with whom to share their personal information,

for what purposes and in exchange for what. As Acquisti et al. [2, p. 445] point out, "privacy is not the opposite of sharing - rather, it is control over sharing".

The data-control view of privacy seems to better account for the individuals' behaviors in the digital society. Actually, even when they are made aware of the potential risks for privacy, individuals are likely to share their personal information (including also very sensitive data, such as their address, phone number, location data, or political preferences) quite easily with other individuals [29], and sometimes even with commercial organizations.

Many authors have observed the incongruence between the high levels of privacy concerns individuals declare and their online behaviors and refer to it as the 'privacy paradox' [8, 33]. Among the explanations of the paradox, the rational-choice argument is one of the most cited: even when they are aware of the risks for their privacy, individuals disclose personal information because the benefits of doing outweigh the cost or risks. This argument is the basis for the so-called 'privacy calculus' [14, 42] individuals are supposed to resort to when requested to provide personal information in exchange for some kind of compensation.

However, while there are evidences that a compensation based strategy can work in transactions between individuals and firms, it is highly disputable that public sector organizations can resort to it to obtain the data subjects' consent to collect their personal information, to use it and (possibly) to make it available for third parties' re-use. In fact, PSOs can offer neither economic compensation to the data subjects in order to make them willing to disclose their personal information in absence of legal obligations, nor non-monetary benefits specifically delivered to them (since this would contradict the principle of impartiality).

What strategies, then, could PSOs implement to make the data subjects willing to consent to the processing (including the possible re-use) of their personal information in the absence of a legal obligation to do that?

4 Unlocking the Value of PSPI

Economic compensation and benefits are not the only elements individuals can consider in deciding whether to disclose their personal information. Recent studies show that the sense of 'psychological ownership' [35, 34] represents an important driver, maybe the most important one, of the individuals' personal information valuation over and above information sensitivity and privacy concerns [48]. Based on an empirical research, Cichy et al. [12] found that the willingness to disclose personal information increases if individuals perceive this as a way to "express themselves, enhance their self-efficacy or contribute to their self-identity by supporting a greater good as a direct consequence of disclosing their personal data" (p. 5).

Psychological elements play a role also in motivating the individuals' disclosure behaviors on social media. Lee et al. [25] found that information disclosure on social media is related to self-clarification, social validation, relationship development, social control, and self-representation. Lutz and Strathoff [29] observe that the use of

social networks represents a form of post-traditional community building individuals resort to foster their relationships and search for a feeling of belonging.

Quite interestingly, the determinants of psychological ownership that have been found to influence the individuals' disclosure behaviors on social media can also motivate the individuals' willingness to be involved as coproducers in the firms' value-producing processes. Starting from the seminal work of Prahalad and Ramaswamy [36], the individuals' involvement as coproducers in value-producing processes has been studied quite extensively within the marketing literature, also with respect to the psychological implications of coproduction for customers' satisfaction [9]. Fuchs et al. [18] found that customers involved as coproducers experience higher levels of psychological ownership than customers who do not participate in the production and delivery processes. Etgar [17] observes that the psychological benefits (potentially) deriving form coproduction include excellence, autonomy, self-expression and uniqueness, enjoyment and self-confidence, as well as status and social esteem (p. 102). These are the same psychological elements that have been found to motivate the individuals' online disclosure behavior. This suggests the possibility of considering coproduction as a possible strategy PSOs can implement to unlock the value of PSPI under the PSI-reuse principle.

The reuse principle makes PSI available to third parties (individuals and organizations) as a resource they could use in their value-producing processes. For PSOs, enabling the reuse of PSI is part of an administrative macro-process that aims at enabling the creation of social value (economic growth and community well-being) by supporting the value-producing processes of public and non-public subjects. When this administrative macro-process uses personal information as a resource, the individuals that information pertains to, and that consent to the use of that resource, should be considered as involved in the process as the providers of a critical resource. Within the public services literature, this is considered as a form of participation in which the users play an active role in the coproduction of value by contributing relevant resources [10] in terms of time, expertise and effort [27], but also compliance and information [4].

Alford [3] observes that the willingness to coproduce is difficult to foster through specific material rewards that are exchanged for the performance of specifically defined tasks. Non-material rewards such as sense of self-determination and competence, sense of belonging to a group (which can be related to some of the determinants of psychological ownership) appear to be more effective as motivators of coproduction behaviors. Besides these, the willingness to contribute to the well-being of other people and towards society at large is an important element of the concept of coproduction in the public sector [5]. Verschuere et al. [52] observe that in order to motivate an individual to engage in coproduction, the issue at hand needs to be of salience to him, where salience may be related also to a concern for community related benefits. Similarly, Bovaird and Löffler [11] observe that there is a huge latent willingness of citizens to act as public services coproducers, but only if they feel that a value for people is created through coproduction.

How can PSOs leverage the motivators of coproduction to unlock the value of PSPI?

The World Economic Forum [54, 55] identified three conditions that need to be satisfied to unlock the value of personal information in a user-centric personal information ecosystem: deliver meaningful transparency, strengthen accountability and empower individuals. Deliver meaningful transparency means to make transparency practices more meaningful, actionable and relevant for individuals by simplifying the ways in which organizations communicate their data practices and presenting individuals with understandable and relevant information on how their information is being used. Strengthen accountability means linking accountability to the impact of different data uses on individuals, and distributing risks equitably among all the stakeholders (not only on the individuals who give the consent to the collection of their data). Empower individuals means giving them a say in how their data is used and engaging them in understanding (and managing) the intended impact of data usage.

Quite interestingly, the three conditions above can be related to the conditions that according to Prahalad and Ramaswamy [36] could facilitate cocreation experiences, i.e. Dialogue, Access, Risk-benefits assessment, and Transparency (the so-called DART framework). Dialogue implies interaction, the willingness to avoid opportunistic behaviors and to recognize an active role to the consumers. Access, implies granting consumers the direct access to information relevant for informed decision-making. Transparency implies reducing the information asymmetry between consumers and firms through the sharing of information. Finally, dialogue, access and transparency make consumers aware of the potential risks of goods and services, so that they can assume more responsibility for dealing with them.

In a user-centric personal information ecosystem, open dialogue and interactivity allow data-subjects, conceptualized as coproducers, to get a clear understanding of how their personal information is collected, used and, possibly, made available for re-use. Giving individuals direct access to the information concerning the use of their data enables the empowerment of individuals and allows them to assume responsibility on the disclosure of personal information and to share with the data collectors the risks involved in the use of their information, as entailed by the same idea of user-centric personal information ecosystem. Pursuing transparency is a way to reduce the information asymmetry between individuals and the organizations that collect and use their personal information. Through transparency, individuals can be made aware of not only how and by whom their personal information is used, but also of what value has been generated by using that information.

Important as it is for reducing the information asymmetry, the control on how personal information is re-used by third parties is a critical activity that would require the data subjects to engage in complex and burdensome data tracking activities, which cannot be reasonably expected. A possible solution to this problem can be based on PSOs playing an information stewardship role within the personal data ecosystem, on behalf of the data subjects. As a component of data governance, information stewardship focuses on assuring accuracy, validity, security, management, and preservation of information holdings [13, p. 380]. Acting as information stewards, PSOs can define data governance policies and implement information management tools that allow them to monitor, and report to the data subjects, how third parties reuse

their personal information. By integrating the data stewardship role within the open, transparent and interactive dialogue with the data subjects, PSOs can assure them that the third parties' reuse of PSPI complies with agreed upon rules, is fair and not purely opportunistic, which is a fundamental condition for the data subjects to consent to the reuse of their personal information.

Based on the observations above, it can be concluded that a possible strategy PSOs can resort to for unlocking the value of PSPI through the application of the PSI-reuse principle within a user-centric personal data ecosystem can be based on two pillars. On the one hand, the implementation of measures to foster transparency through open dialogue and information sharing, which includes undertaking the role of information steward. On the other hand, the involvement of the data subjects as coproducers in the decisions concerning whether and at what conditions to make PSPI available for reuse.

5 Conclusions, Limitations and Further Research Directions

In the paper it has been suggested a possible solution for extending the application of the PSI-reuse principle to PSPI in a user-centric personal data ecosystem. The suggested solution depends on two critical conditions PSOs must satisfy. On the one hand, they should involve the data subjects as coproducers in the process that allows the reuse of PSPI, which entails a continuous, open, transparent and interactive dialogue between the two parts. On the other hand, PSOs should act as information stewards on behalf of the data subjects, which entails implementing technological and organizational solutions to assure the data subjects that third parties will not use their personal information opportunistically.

Both conditions require PSOs to implement complex processes of organizational change. Coproduction entails re-balancing the power relationships between public officials and citizens, which affects responsibility and accountability. This explains why, as it is widely discussed within the marketing and the public management literature, there are still many resistances within public organizations toward coproduction. Such resistances can be even stronger if PSOs are required to play a stewardship role on behalf of the data subjects, which entails performing critical activities to monitor third parties' reuse of PSPI and assuming a new responsibility toward the data subjects for how their personal information will be reused by third parties.

The solution suggested in the paper rests critically on the assumption that the right to decide whether, under what conditions and in change for what to disclose personal information to trusted counterparts is actually granted to the data subjects. This principle, which is the foundation of the user-centric personal data ecosystem, has not been fully incorporated yet within the privacy preserving legislation, although the General Data Protection Regulation currently in force in the European Union represents an important step in that direction.

In the paper no distinction has been made among different types of personal information that, as argued in [32], can be associated to different types and levels of perceived risks. This represents a limitation of the present study that needs to be overcome to identify the incentive mechanisms that can be most effective in the different cases.

Finally, the paper has been based exclusively on a conceptual analysis and this is its main limitation. The literature discussed in the paper provides only indirect evidences supporting the hypothesis that a coproduction strategy could motivate the data subjects to consent to the reuse of their personal information. Hence, more research is needed to develop further and to test this hypothesis also based on empirical data.

However, preliminary as it is, the results of the discussion in this paper show that coproduction can play a relevant role to unlock the value of personal information in the emerging user-centric personal information ecosystem.

References

1. AA.VV. (2018). *Study to support the review of Directive 2003/98/EC on the re-use of public sector information—Final Report*, European Union, Brussels.
2. Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442–492.
3. Alford, J. (2002). Why do public-sector clients coproduce? Toward a contingency theory. *Administration & Society, 34*(1), 32–56.
4. Alford, J. (2009). *Public sector clients: From service-delivery to co-production*. Basingstoke: Palgrave Macmillan.
5. Alford, J. (2012). *The multiple facets of co-production*. Building on the work of Elinor Ostrom. Paper for the Seminar on 'Co-production: The State of the Art', Budapest.
6. Allen, A. L. (2000). Privacy as data control: conceptual, practical, and moral limits of the paradigm. *Connecticut Law Review, 32,* 861–875.
7. Andersen, E. (2011). *Prepared statement for the hearing before the committee on commerce, science, and transportation*, United State Senate, March 16, 2011.
8. Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13–28.
9. Bendapudi, N., & Leone, R. P. (2003). Psychological implications of customer participation in co-production. *Journal of Marketing, 67,* 14–28.
10. Bovaird, T. (2007). Beyond engagement and participation: User and community coproduction of public services. *Public Administration Review, 67*(5), 846–860.
11. Bovaird, T., & Löffler, E. (2012). From engagement to co-production: The contribution of users and communities to outcomes and public value. *VOLUNTAS: International Journal of Voluntary and Nonprofit Organizations, 23,* 1119–1138.
12. Cichy, P., Salge, T. O., & Kohli, R. (2014). Extending the privacy calculus: The role of psychological ownership. In *Proceedings of ICIS 2014* (pp. 1–19). AIS-ICIS, Atlanta.
13. Dawes, S. S. (2010). Stewardship and usefulness: Policy principles for information based transparency. *Government Information Quarterly, 27*(4), 377–383.
14. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-Commerce transactions. *Information Systems Research, 17*(1), 61–80.
15. Dwork, C. (2006). Differential privacy. In *Proceedings of 3rd International Colloquium on Automata, Languages and Programming (ICALP)* (pp. 1–12). Berlin: Springer.

16. EDPS. (2016). *EDPS opinion on personal information management systems*. European Data Protection Supervisor, Opinion 9/2016. European Union, Brussels.
17. Etgar, M. (2008). A descriptive model of the consumer coproduction process. *Journal of the Academy of Marketing Science, 33,* 97–108.
18. Fuchs, C., Prandelli, E., & Schreier. M. (2010). The psychological effects of empowerment strategies on consumers' product demand. *Journal of Marketing, 74*(1), 65–79.
19. Golle, P. (2006). Revisiting the uniqueness of simple demographics in the US population. In *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society (WPES'06)* (pp. 77–80). NY: ACM.
20. Graux, H. (2011). *Open government data: reconciling PSI re-use rights and privacy concerns*. European Public Sector Information Platform. Topic Report No. 2011/3.
21. Janssen, K. (2011). The influence of the PSI directive on open government data: An overview of recent developments. *Government Information Quarterly, 28*(4), 446–456.
22. Kang, J. (1998). Information privacy in cyberspace transactions. *Stanford Law Review, 50*(4), 1193–1294.
23. Van Kleek, M., & O'Hara, K. (2014). The future of social is personal: The potential of the personal data store. In D. Miorandi, V. Maltese, M. Rovatsos, A. Nijholt, & J. Stewart (Eds.), *Collective intelligence: Combining the powers of humans and machines to build a smarter society* (pp. 125–158). NY: Springer.
24. Kulk, A., & van Loenen, B. (2012). Brave new open data world? *International Journal of Spatial Data Infrastructures Research, 7*(2), 196–206.
25. Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on social network services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies, 71*(9), 862–877.
26. Liem, C., & Petropoulos, G. (2016). *The economic value of personal data for online platforms, firms and consumers*. LSE Business Review, January 19, 2016.
27. Linders, D. (2012). From e-government to we-government: Defining a typology for citizen coproduction in the age of social media. *Government Information Quarterly, 29,* 446–454.
28. van Loenen, B., Kulk, S., & Ploeger, H. (2016). Data protection legislation: A very hungry caterpillar: The case of mapping data in the European Union. *Government Information Quarterly, 33*(2), 338–345.
29. Lutz, C., & Strathoff, P. (2013). Privacy concerns and online behavior—Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. In S. Brändli, R. Schister, & A. Tamò (Eds.), *Multinationale Unternehmen und Institutionen im Wandel –Herausforderungen für Wirtschaft, Recht und Gesellschaft* (pp. 81–99). Berne: Stämpfli.
30. Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33*(3), 5–21.
31. Meredith, J. (1993). Theory building through conceptual methods. *International Journal of Operations and Production Management, 13*(5), 3–11.
32. Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs, 51*(1), 133–161.
33. Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126.
34. Pierce, J. L., & Jussila, I. (2011). *Psychological ownership and the organizational context*. Cheltenham, UK: Edward Elgar.
35. Pierce, J. L., Kostova, T., & Dirks, K. T. (2003). The state of psychological ownership: Integrating and extending a century of research. *Review of General Psychology, 7,* 84–107.
36. Prahalad, C. K., & Ramaswamy, V. (2004). Cocreation experiences: The next practice in value creation. *Journal of Interactive Marketing, 18*(3), 5–14.
37. Pyrozhenko, V. (2017). Open government: Missing questions. *Administration & Society, 49*(10), 1494–1515.
38. Scassa, T. (2014). Privacy and open government. *Future Internet, 6,* 397–413.

39. Shmatikov, V., & Narayanan, A. (2010). Myths and fallacies of 'personally identifiable information'. *Communications of the ACM, 53*(6), 24–26.
40. Simpson, A. C. (2011). On privacy and public data: A study of data.gov.uk. *Journal of Privacy and Confidentiality, 1*, 51–65.
41. Sloot, B. (2011). Public sector information & data protection: A plea for personal privacy settings for the re-use of PSI. *Informatica e Diritto, 1–2,* 219–236.
42. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 99–1015.
43. Sobolewski, M., Mazur, J., & Paliński, M. (2016). GDPR: A step towards a user-centric internet? *Intereconomics, 52*(4), 207–213.
44. Solove, D. J. (2002). Access and aggregation: Public records, privacy and the constitution. *Minnesota Law Review, 86,* 1137–1209.
45. Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–560.
46. Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review, 126*(7), 1880–1904.
47. Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K. (2015). The challenges of personal data markets and privacy. *Electronic Markets, 25,* 161–167.
48. Spiekermann, S., & Korunovska, J. (2016). Towards a value theory for personal data. *Journal of Information Technology*. https://doi.org/10.1057/jit.2016.
49. Sweeney, L. (2006). *Uniqueness of simple demographics in the U.S. Population*. Carnegie Mellon University.
50. Tene, O. (2011). Privacy: The new generations. *International Data Privacy Law, 1*(1), 5–27.
51. Thaler, R. H., & Tucker, W. (2013). Smarter information, smarter consumers. *Harvard Business Review, 91,* 45–54.
52. Verschuere, B., Steen, T., Van Eijk, C., & Verhaeghe, T. (2014). *Motivations for coproduction of public services: Empirical evidence from a comparative case study*. Paper presented at the *IIAS* Study Group on Coproduction of Public Services Meeting. Bergamo, IT.
53. WEF. (2011). *Personal data: The emergence of a new asset class*. World Economic Forum, Geneva.
54. WEF. (2013). *Unlocking the value of personal data: From collection to usage*. World Economic Forum, Geneva.
55. WEF. (2014). *Rethinking personal data: A new lens for strengthening trust*. World Economic Forum, Geneva.
56. Westin, A. F. (1967). *Privacy and freedom*. NY: Athenum.
57. Wiebe, A., & Dietrich, N. (2017). *Open data protection study on legal barriers to open data sharing—Data protection and PSI*. Göttingen: Universitätsverlag Göttingen.
58. Zuiderwijk, A., & Janssen, M. (2014). Open data policies, their implementation and impact: A framework for comparison. *Government Information Quarterly, 31*(1), 17–29.
59. Zuiderwijk, A., & Janssen, M. (2014). The negative effects of open government data—Investigating the dark side of open data. In *Proceedings of the 15th Annual International Conference on Digital Government Research* (pp. 147–152). New York: ACM.