Will, Matthias Georg

Working Paper

Privacy and Big Data: The need for a multi-stakeholder approach for developing an appropriate privacy regulation in the age of Big Data

Diskussionspapier, No. 2015-3

Provided in Cooperation with:
Martin Luther University of Halle-Wittenberg, Chair of Economic Ethics

Suggested Citation: Will, Matthias Georg (2015) : Privacy and Big Data: The need for a multi-stakeholder approach for developing an appropriate privacy regulation in the age of Big Data, Diskussionspapier, No. 2015-3, ISBN 978-3-86829-771-3, Martin-Luther-Universität Halle-Wittenberg, Lehrstuhl für Wirtschaftsethik, Halle (Saale), https://nbn-resolving.de/urn:nbn:de:gbv:3:2-46372

This Version is available at:
https://hdl.handle.net/10419/170436

Matthias Georg Will

Privacy and Big Data: The Need for a Multi-Stakeholder Approach for Developing an Appropriate Privacy Regulation in the Age of Big Data

Discussion Paper No. 2015-03

of the Chair in Economic Ethics,
Martin-Luther-University Halle-Wittenberg,
edited by Ingo Pies,
Halle 2015

Disclaimer

The publications in this series of Business Ethics studies provide a platform to promote discourse and learning. Therefore, the views, ideas and opinions do not necessarily reflect those of the editor. The authors themselves are and remain accountable for their statements.

ISBN 978-3-86829-770-6 (printed version)
ISBN 978-3-86829-771-3 (electronic version)
ISSN 1861-3594 (printed version)
ISSN 1861-3608 (electronic version)

Authors' contact details

Dr. Matthias Georg Will
Martin-Luther-University Halle-Wittenberg
Faculty of Law, Economic and Business
Economic Department
Chair in Economic Ethics
Grosse Steinstrasse 73
D-06108 Halle – Germany
Tel.: +49 (0) 345 55-23357
Tel.: +49 (0) 345 55-23421
Email: matthias.will@wiwi.uni-halle.de

Address for correspondence

Dr. Matthias Georg Will
Martin-Luther-University Halle-Wittenberg
Faculty of Law, Economic and Business
Chair of Economic Ethics
Große Steinstraße 73
06108 Halle – Germany
Tel.: +49 (0) 345 55-23357
Fax: +49 (0) 345 55 27385
Email: matthias.will@wiwi.uni-halle.de

Abstract

This paper presents a multi-stakeholder approach for developing an appropriate privacy regulation in the age of big data. We develop our argument in five steps, starting (1) with a review of the current academic debate on privacy regulation. We analyze a dysfunctional mutual excludability between the suggestions of the supporters of a regulation orchestrated by governments, and the supporters of internet self-regulation. (2) To overcome this conflict, we argue that the framework for developing an appropriate privacy regulation should not only focus on formal and procedural aspects (e.g., who might develop and implement it) but should also include some important substantial aspects to protect users and promote socially beneficial big data applications. (3) After examining substantive aspects of a functional privacy regulation, we examine how the process leading to an appropriate regulation might be organized. In addition, we discuss how an organization might be designed to conduct this process. In our argument, stakeholder dialogues and an independent "privacy organization" are relevant parameters. (4) We discuss the potential structure of a privacy organization that might conduct multi-stakeholder-dialogues as a preliminary step. This organization could then govern and monitor the implementation of a privacy regulation that was defined by the stakeholder dialogues. (5) Finally, we discuss our findings and suggestions.

Key words: Big Data, Privacy, Regulation, Stakehoder Dialgues, Multi-Stakeholder Approach, Transaction Costs, Property Rights

Kurzfassung

Dieser Beitrag stellt einen Multi-Stakeholder-Ansatz vor, um eine funktionale Regulierung für den Datenschutz im Big-Data-Zeitalter zu entwickeln. Die Argumentation wird in fünf Schritten entwickelt: (1) Zuerst wird die aktuelle internationale akademische Debatte hinsichtlich des Zusammenspiels von Big Data und Datenschutz kurz skizziert. Dieser Beitrag arbeitet einen für die Regulierung dysfunktionalen Konflikt zwischen den Vorschlägen der Befürworter einer staatlichen Regulierung und den Anhängern einer Internet-Selbstregulierung heraus. (2) Ein Ansatz für eine geeignete Regulierung der Privatsphäre sollte nicht ausschließlich formal-rechtliche Aspekte berücksichtigen, wie z. B. wer die Regulierung entwickeln und umsetzen sollte, sondern auch materielle Aspekte berücksichtigen, um Nutzer zu schützen und die gesellschaftlichen Vorteile von Big-Data-Anwendungen zu fördern. (3) Hierauf aufbauend präsentiert dieser Beitrag formal-rechtliche Überlegungen, wie eine geeignete materiell-rechtliche Regulierung erreicht werden kann. In diesem Zusammenhang wird diskutiert, wie eine Organisation gestaltet werden kann, um diesen Prozess zu unterstützen. Hierfür sind Stakeholder-Dialoge und eine unabhängige „Privacy Organization" erforderlich. (4) Im Anschluss präsentiert dieser Aufsatz, wie die Organisationsstruktur einer „Privacy Organization" geschaffen sein kann und wie diese als einen ersten Schritt einen Multi-Stakeholder-Dialog durchführen kann. Diese Organisation kann auch die Umsetzung der durch die Stakeholder-Dialoge gefundene Regulierung begleiten und überwachen. (5) Abschließend werden die Erkenntnisse und Vorschläge dieses Beitrages diskutiert.

Schlagwörter: Big Data, Datenschutz, Regulierung, Stakeholder Dialoge, Mutli-Stakeholder Ansatz, Transaktionskosten, Eigentumsrechte

JEL classification: K11, K19, K20, K33, L5, L14

Privacy and Big Data: The Need for a Multi-Stakeholder Approach for Developing an Appropriate Privacy Regulation in the Age of Big Data

Matthias Georg Will*

Introduction

As many researchers point out, big data generates an enormous number of opportunities in many diverse fields of endeavor. For example, big data applications may revolutionize the whole health care system through analyzing risk profiles, the effect of drugs or unforeseen adverse reactions (Tene and Polonetsky, 2012, p. 64, Tene and Polonetsky, 2013, pp. 245-247, Chen et al., 2012, pp. 1173, Table 2). Other applications include smart grids that help save energy by more efficient structuring of the complex energy supply and demand network (Tene and Polonetsky, 2012, p. 64, Tene and Polonetsky, 2013, p. 248). Big data may also reduce traffic jams, road deaths and improve fuel-efficient driving (Tene and Polonetsky, 2012, p. 64, Tene and Polonetsky, 2013, p. 248). It may also give rise to many opportunities in second and third world countries as new and cheaper solutions are developed that address the needs of the bottom billion (Tene and Polonetsky, 2013, p. 247). The benefits may range from access to better education to relevant information about climate- and soil-specific cultivation methods, or information about diseases that mainly occur in second and third world countries.

In addition, big data enables investigators to reduce fraud by controlling financial transactions in real time, or warn potential victims of criminal intent (Tene and Polonetsky, 2013, pp. 249-250). Big data may also be applicable for some crimes (like burglary) that seem to follow specific patterns (e.g., time of day, weather, district, etc.). Data mining can reveal these patterns and inform police where and when the greatest probability of criminality may occur (Adderley, 2004). The application of big data to fighting terrorism may lead, for example, to the exposure of sleepers (Chen et al., 2012, pp. 1173, Table 2).

The use of big data in the corporate world could increase efficiency within the retail business (Iansite and Lakhani, 2014, Tene and Polonetsky, 2012, p. 65, Tene and Polonetsky, 2013, p. 249). Companies could apply data mining to gauge their customers' behavior based on various parameters. Big data may also revolutionize the management of organizations, e.g., the availability and ease of analysis of data gives managers profound information about complex interactions within their organizations (Iansite and Lakhani, 2014, Davenport et al., 2012, LaValle et al., 2011, McAfee and Brynjolfsson, 2012). Management would then become more familiar with relevant interdependencies that cannot be revealed without big data (e. g. increase resource efficiency, optimize the utilization capacity, connect market research with research and development in a more efficient way, etc.). Needless to say, internet companies would also benefit extremely well through big data applications (Iansite and Lakhani, 2014, Pentland, 2014, Tene and Polonetsky, 2013,

* The authors declare that there are no conflicts of interest. The authors financed this reply with internal resources. We acknowledge constructive comments from Stefan Hielscher, Ingo Pies, Walter Precht (http://walter-precht.de/) and Jan Winkin.

pp. 250-251), e.g., they could optimize their search engines or social networks and use the data for target-group-specific services on both sides of the markets they address.

However, there is a dark side to big data – its abuse or exploitation for socially undesirable or at least questionable purposes by companies, governments and criminals. The abuse of big data erodes fundamental privacy laws (Boyd and Crawford, 2012, pp. 671-673, Tene and Polonetsky, 2012, p. 65, Tene and Polonetsky, 2013, pp. 251-252). Historically, anonymous use of private data should have been a reasonable protection against data theft or data abuse, however, big data enables a re-identification of anonymized data. In addition, there are many ethical issues surrounding the use of big data that are still open for public debates: e.g., do we want to receive personalized ads and if so, how often (Tene and Polonetsky, 2013, pp. 252)? As a society, do we really want predictive analysis for crime ("pre-crime") and illness, because predictive analysis may stigmatize individuals and neighborhoods (Tene and Polonetsky, 2013, pp. 253-254)?

Furthermore, big data may lead to monopolies within the business sector: companies that rarely use big data may go bankrupt, whereas other firms survive because they apply data mining on a large scale (Tene and Polonetsky, 2013, pp. 254-255). This may lead to global oligopolies or monopolies with disastrous consequences for consumers and society in general. In addition, the ease with which big data can be accessed may encourage some people to abuse the data, merely because it is technically possible (e.g., hackers) (Tene and Polonetsky, 2013, pp. 256). Finally, the big data paradigm may subliminally influence our behavior (Tene and Polonetsky, 2013, pp. 256). If people know that big data (as in the Orwellian "Big Brother") enables third parties to find out everything about everyone, preemptive obedience may ruin individualism and freedom. However, liberal societies are based on the general principle of the individual's right to privacy that protects them from others (including governments).

The above overview of the opportunities and risks of big data begs the question "How do we – as a (world) society – want to manage the ambivalence of big data"? (1) The first section summarizes the academic debate on the regulation of big data and privacy. We highlight how this debate perceives the alternatives of regulating big data as mutually excludable measures. This mutual excludability prevents finding adequate solutions for overcoming the ambivalence of big data. (2) We present some considerations for developing solutions that might overcome the analyzed deficiencies of the debate. These considerations have to be fulfilled by a well-designed regulatory regime. The present considerations, from a legal standpoint, can be seen as criteria for the substantive side of a privacy regulation. (3) We show in the third section how a well-designed multi-stakeholder dialogue may be the right context for developing further privacy regulation on a global scale. We present some arguments that address the formal side of an appropriate privacy regulation. (4) Against this backdrop, we describe an organization that effectively organizes and implements this multi-stakeholder framework. (5) In conclusion, we discuss the findings of our paper.

1. The Academic Debate on Privacy and Big Data Regulation

An appropriate regulatory framework for big data should not cause conflict with opportunities promised by big data. A well-designed framework would even promote such opportunities, minimize private and social risks, bring together the varying interests of individuals, researchers, firms and authorities, while efficiently inhibiting the socially undesirable data theft or abuse by private or governmental actors. Potential benefits and problems of data abuse are intimately linked with privacy issues, specifically those limiting access to personal information and the right of having secrets or the control over others' use of personal information (Solove, 2008, pp. 12-13).

The big challenge to designing an adequate regulatory framework is that traditional concepts of privacy have failed in the age of big data (Tene and Polonetsky, 2013, pp. 257-263). Principles like de-identification, data-minimization and individual control are no longer practicable and enforceable and this has led scholars to demand a new regulatory framework (Weber, 2010, Tene and Polonetsky, 2012, p. 69, Tene and Polonetsky, 2013, pp. 257-263, Goldsmith, 1997-1998, Schwartz, 2000).

To meet private and societal interests through better regulation of big data, the academic debate concentrates on two different regulatory approaches that seem to be mutually excludable: (1) self-regulation of the internet (actors), and (2) governmental regulation that sets the framework for big data applications (cf. Schwartz, 2000, pp. 815-816).

(1) *Approaches of self-regulation*: Schwartz (2000, p. 816) argues that many activists and supporters of the internet are in favor of a self-regulation and are strongly against a state-led regulation. He summarizes the standpoint of the supporters of a self-regulation in an ironic way: "Faced with these choices, only someone with nostalgia for Soviet-style central planning would disagree with the conventional wisdom that we should favor the market, bottom-up decision-making, and self-regulation in cyberspace. From this perspective, the role of the State, if not nonexistent, is to be as constrained as possible." The perspective of many internet activists and supporters seems plausible from an historical perspective because of the enormous benefits that ordinary people have gained from a self-regulated or poorly regulated internet: people perceive the internet as a place that is free from governmental despotism. This perspective is also supported by the fact that the internet has never been limited to one nation, but is, rather, a global institution that connects people all around the world independent of their national background. Government regulation, therefore, looks antagonistic to many internet activists and supporters.

Even if the idea of self-regulation seems compatible with the extremely dynamic structure of the internet, self-regulation entails some risks and dangers for all users (including firms). The internet community has not yet developed an appropriate self-regulating framework for big data: different forms of data abuse continue to pose a risk, including that from (multi-national) corporations using their data for socially undesirable applications. Furthermore, governments are also using big data (applications) with little or non-existent oversight by civilian bodies. Finally, even if there were a self-regulatory framework, it is unclear what organization could enforce

its implementation and sanction violators.

(2) *Approaches of governmental regulation*: Supporters of regulation by nation states argue that nation states can and should regulate the internet (Weber, 2010, p. 30, Schwartz, 2000, p. 858, Goldsmith, 1997-1998, pp. 1119-1122). These supporters argue that the internet is not an extraterrestrial place: servers are located in national jurisdictions and so are the internet users. Although nation states can, of course, develop an internet regulation, multi-national initiatives would be required to handle special issues that concern more than one country.

However, government regulation of big data may also prove to be dysfunctional imposing additional risks to society. The national regulation of privacy is far from being satisfactory and there is little evidence that nation states would handle the challenge of big data and individual privacy in any meaningful way. In addition to these deficiencies, enormous amounts of data are quickly and easily moved through the internet, e.g., regardless of national borders. Thus, an adequate privacy regulation would require a multi-national framework, one which is not presently workable. Another argument against national regulation is the risk that it would be influenced by national commercial policies, jeopardizing, e.g., the privacy interests of non-nationals. National regulation may also reduce the social (net) benefits of innovative big data applications because of a dysfunctional overregulation when state regulators attempt to control technological developments associated with big data. This over-regulation may be driven by a biased overestimation of the dangers and an underestimation of the social gains of innovations.

	Solely Governmental Regulation	*Solely Internet Self-Regulation*
Societal Aims:	Using Big Data in a Socially Desirable Way	Using Big Data in a Socially Desirable Way
+ Δ Constraints:	New and better Governental Regulation	Implent Internet Self-Regulation
⇒ Possibly Dysfunctional Societal Outcome:	Missing Accrediaton, Arbitrary Policies, and Restricing Freedom	Monopolization, Data Abuse

Figure 1: The mutual excludability of alternatives for privacy regulation within the academic literature (based on Homann, 1985, p. 53-54, Pies, 2009, p. 10)

Figure 1 illustrates the underlying logic of the alternatives to privacy regulation as discussed within the academic literature. There seems to be an underlying assumption that the social aims of big data (increasing the opportunities and reducing the risks) can be reached either through self-regulation or government regulation.

However, this perception of the regulatory alternatives has many deficits because scholars argue in a way that regulatory measures seem to be mutually excludable. Because of this argumentation in both camps, neither governmental regulation nor internet self-regulation might be appropriate for reaching the societal aims:

(a) governmental regulation (as the supporters of self-regulation argue) may lack international accreditation and may be susceptible to arbitrary national industrial policy. In addition, a governmental regulation of the internet may restrict individual freedom rights in less democratic countries.

(b) In contrast, internet self-regulation (as the supporters of governmental regulation argue) may be ineffective in preventing a propensity toward monopolization and data abuse.

Neither governmental regulation nor self-regulation, from this perspective, would seem to be appropriate for a regulatory framework that increases the benefits of big data and limits its risks and dangers at the same time. Both mutually excludable measures may have negative consequences and, thus, result in poor regulation.

Tene and Polonetsky (2013, pp. 263-270) recommend a set of guidelines that a regulation for privacy should contain, which go far beyond the perception of the regulatory alternatives noted above. They develop some substantive arguments for a better regulation independent of the body charged with implementing these measures.

First, the authors contend that internet users need extended access rights including free access to their data. In addition, users should benefit from different features that allow them to enhance their data. Companies or even third-party suppliers shall offer a "featurization" of personal data, the rationale being that users should be compensated for the corporate value that is generated by their private data. However, both authors point out that extended access rights and featurization are complicated and may cause high transaction costs.

In addition, the two authors suggest that a regulation has to create a transparent environment in which secret databases are forbidden: an appropriate regulation would then ensure enhanced transparency (Tene and Polonetsky, 2013, pp. 270-272), including the idea that firms publish the reasons behind their decisions or policies, but, not disclosing the algorithms that companies use for analyzing their data. Tene and Polonetsky (2013) also note a major flaw in the privacy/big data debate: if users are uninterested and disengaged, privacy – even well-regulated – becomes a moot point.

We note that Tene and Polonetsky (2013), although having a strong focus on self-regulation, do not discuss who might be responsible for implementing the new regulation and how it should be done. In summary, Tene and Polonetsky (2013) present ideas that primarily focus on the function of the regulatory measures and not whether governments or internet actors should implement them. Conceptually, their reasoning attempts to overcome the limitations of the mutual excludability associated with internet regulation at first glance, but, their ideas may be difficult to implement at second glance. Thus, despite of their substantive suggestions, their ideas may fail in overcoming the above regulatory excludability because of the difficulties of implementing.

We suggest that we can make Tene and Polonetsky's (2013) recommendations more fruitful through a more systematic analysis of the underlying problems that create the need for a well-designed regulatory framework that better protects privacy. In the next section, we attempt to clarify some of the underlying problems in order to develop a preliminary blueprint for an appropriate regulation that will neutralize the above conflicts between proponents of an internet self-regulation and the supporters of a governmental regulation. In this section, we analyze the substantive assumptions for an appropriate privacy regulation.

2. Transaction Costs and an Appropriate Regulation of Privacy and Big Data

From a public policy perspective, the distribution and design of privacy regulation may have an impact on the allocation (e. g., how we use big data and who uses big data) and its social consequences (e. g. if big data applications have socially desirable or undesirable consequences) (Coase, 1960). The decisive factor for the allocation and the social consequences are transaction costs. As we will argue, transaction costs are not just a given and irrevocable factor. Instead, the design of a regulatory regime can influence transaction costs. We first summarize Coase's (1960) approach and then adapt this argument to privacy regulation for analyzing relevant issues considering the distribution and design of property rights on (private) data. This helps overcome the negative aspects of previous approaches to regulating privacy and big data.

(1) *Transaction costs, property rights and welfare*: Coase (1960) makes some assumptions to develop his famous argument. First, resources are scarce and property rights exist in order to properly distribute these scarce resources. Second, the use of these resources has social consequences: the actions of some people may harm third parties whereas the actions of others are of benefit to third parties. Third, property rights of the scarce resources can be transferred from one party to another. Fourth, if transaction costs (e.g., the time and effort involved in finding appropriate transaction partners or signing valid contracts, etc.) do not exist, it is costless to transfer property rights. In the initial situation (where there are no transactions costs), although surprising, it does not matter in terms of social welfare who gets the property rights. The argument is that people will transfer property rights as long as the property rights are distributed in a way that maximizes the social good. Fifth, now let's assume that transaction costs exist. In this case, the distribution of property rights is of importance because these costs may limit parties transferring property rights even if this would increase the social good. As a consequence, the exchange of property rights and resulting benefits to society are restricted in a world with transaction costs.

(2) *Privacy, transaction costs and the benefits of big data*: Potential regulatory regimes vary, e.g., from a situation in which (private) users have full control over their data, to a situation in which data are a common resource. Users in the latter case would not be able to decide who uses their data nor how it might be used. We would contend that the relevant questions are (a), who holds property rights over private data and (b), how are these property rights designed.

(a) *The distribution and enforceability of privacy*: Following Coase's (1960) approach, the design of a regulatory framework for privacy predetermines who, initially, has the property rights on private data and to what extent privacy is enforceable. As a consequence, enforceable property rights on private data may promote the positive effects of big data or – in the case of unenforceable rights – enable companies or governments to abuse big data.

(b) *The relevance of transaction costs for transferring private data*: In addition, the design of the property rights influences the amount of monetary and non-monetary transaction costs that would arise if parties want to transfer private data. A poor framework that leads to high transaction costs (and consequent difficulty in transferring property rights) may cause an underutilization of big data (for example less research because users are not willing to transfer data). High transaction costs may also result in abuses of big data because users can hardly protect their privacy if they have released their data once.

Thus, a well-designed regulatory framework has to consider the distribution of

property rights on private data and the transaction costs that arise when parties want to transfer private data. We can, therefore, examine three substantive factors that are influencing the extent to which private data are used for socially desirable applications or for the opposite:

(a) *The transfer of property rights on private data*: The most obvious transaction costs emerge when users and companies negotiate which personal data may be collected by the company and how these data might be used. The following example focuses on the issue of high transaction costs influencing the social effects of transferring property rights of private data. This example also illustrates how the design of the regulatory regime can influence the extent of these costs. In addition, the example shows that a regime with lower transaction costs may cause additional disadvantages as a negative side-effect of this regime, which have to be balanced with the gains of lower transaction costs.

Typically, the exchange of property rights on private data between users and companies is organized through general business terms over which users are rarely allowed any input. This, initially, does not appear very customer-friendly. From a transaction-cost perspective, this appears in a different light because of an underlying tradeoff: companies and users could attempt to negotiate every single interaction causing high transaction costs and reducing the mutual gains of big data. Focusing on the mutual benefits might be a practicable solution compared to individual negotiations. This argument is based on the special business model of many internet firms: these companies focus on innovative solutions for two-sided markets. On the consumer side, the company exchanges "free" (or extremely cheap) services in return for user data. On the business-to-business (b2b) side of the market, the company offers services for third parties by developing valuable big data applications that are based on the users' data. High transaction costs would tremendously increase the costs of these business models and, as a consequence, reduce the availability of "free" services for consumers and valuable big data applications for the b2b side of the market. If the firm and its customers accept standardized business terms that reduce the transactions costs, the potential benefits of big data applications increase for every party. However, standardized business terms offer little choice to the users who cannot negotiate solutions that fit their personal preferences. Users have to balance the potential benefits of using these "free" services versus the grief of accepting standardized business terms: users can either accept the business terms or refuse the service.

Generally speaking, transaction costs emerge when the supply and demand sides of a market fail to negotiate easily appropriate contracts for the involved parties. Historically, we have developed many social and technical innovations to reduce transaction costs in markets (e.g., fiat money, civil law, stock markets, the internet, etc.). Technological or governance innovations could also decrease transaction costs involved with big data if actors want to exchange property rights. This provides a focus for further research. General business terms are just one very simple governance innovation how to reduce transaction costs. However, this governance structure brings up the disadvantage that users can only accept or reject.

(b) *The enforceability of privacy rights*: Another issue for the handling of big data is the enforceability of property rights on private data. Personal data can easily be copied and transferred without permission: secret databases may store private data

also without permission (Tene and Polonetsky, 2013, pp. 263-270). In addition, companies can transfer private data to other jurisdictions to circumvent national privacy laws. Thus, the idiosyncrasy of data and the technical possibilities (for abuse) make it difficult for users to enforce property rights over their private data. Users may, accordingly, restrict the amount of data that they are willing to make available even if companies are apparently trustworthy and have socially beneficial business ideas. Socially beneficial research and development using big data applications is consequently hindered.

Against this backdrop, one might think that the precautionary principle might be an appropriate solution in a world in which privacy rights can hardly be enforced. In this context, the precautionary principle would mean that bureaucrats would only allow big data applications if abuse can be absolutely excluded by the firm. However, the social disadvantages may outweigh the additional security for private data. Even socially desirable innovations may be blocked because it cannot be precluded that the intended innovation is completely risk-free (Pies, 2012, pp. 4-5). Considering this , the precautionary principle might prevent nearly every innovation in the field of big data.

(c) *The value of private data*: Another obstacle to efficient transfer of private data may be its monetary assessment. The marginal value of private data may be low, however, its value as part of a bigger picture may be exponentially higher because of the gains through data mining. Data mining may cause enormous network externalities and thus drive the value of the whole data set even if the single data point is nearly worthless. As an example, Google or Facebook can collect private data, cheaply, which, when aggregated, on the other market side – the b2b-side – become extremely valuable.

However, the relatively poor compensation to users (because of the marginal value of data) may cause users to think that they are being unfairly treated. Consequently, they might boycott big data firms and support populist political solutions to enforce stricter regulation (and/or higher taxation) of big data firms. However, all these measures may be counterproductive to the social gains generated by big data: entrepreneurs, e.g., would not get to experience the thrill of implementing innovations. This has negative consequences for consumers, firms and the society as a whole.

By focusing on the gap between marginal and average value, Tene and Polonetsky (2013, pp. 263-270) suggest a featurization of the big data gains to compensate users adequately. Unfortunately, this would cause additional (transaction) costs for big data firms because of the need to continuously reevaluate the gap between marginal and partial values of individual data. Additionally, they would have to offer interesting features for compensating the internet users. However, the higher additional costs may also lead to less innovations in the field of big data.

Summarizing the social consequences of the above measures that try to reduce this gap between marginal and average values of private data, we argue that the measures for achieving a "fair" compensation of internet users at the b2c-side have negative side effects that may outweigh an additional compensation of this group. These measures increase the transaction costs to big data firms who may lose interest in developing innovative big data solutions.

Summarizing the above findings, we argue that an efficient and effective privacy

regulation has to find solutions to issues associated with, e.g., transferability of property rights to private data, the enforceability of privacy rights and the value of private data. We present in the next section a multi-stakeholder approach that may be the blueprint for an appropriate regulatory framework for the age of big data. This stakeholder approach might consider the above substantive findings for developing an appropriate internet regulation in the age of big data.

3. A Multi-Stakeholder Framework for Governing Privacy in the Age of Big Data

What does an appropriate regulatory framework look like that is able to overcome the deficiencies of traditional privacy regulation and protects users against data abuse without relinquishing the (potential) gains of big data? By presenting our multi-stakeholder framework, we show that it is possible to create benefits to society through big data and to protect privacy at the same time. A functional regulation of privacy and big data is necessary in this framework. This approach builds on the assertion of Tene and Plonetsky (2012; p. 56) that we need a solution that integrates the interests of researchers, companies and users.

Many scholars in the field have expressed the need for a (global) multi-stakeholder dialogue in order to develop a suitable framework for the management of privacy and big data. For example, Baird (2002) argues that a global "round table" may be necessary for a functional regulation of the internet. He adds that openness and accountability of this "round table" are important process criteria for developing an effective internet regulation acceptable to all parties. Similarly Hill (2014) argues that a multi-stakeholder dialogue is necessary for designing an appropriate regulation of the internet.

A multi-stakeholder discourse would focus on developing solutions for safe data retention, data processing that is in-line with ethical standards, and a classification of legal options for data transfer to third parties. In addition, a set of ethical standards could be defined that give a framework for the use of big data applications in business, science and governments. This framework may also define the users' rights to their data and the duties of the data storing, processing and transferring organizations. Several procedural requirements need to be fulfilled to achieve a successful regulation framework: (1) an independent organization has to be established that (2) develops an appropriate design for multi-national stakeholder dialogues. (3) Companies and governments have to implement the results of the stakeholder dialogues. Therefore, monitoring and sanctioning may be necessary.

(1) *The need for an independent organization*: We believe that both nation states (a) and companies (b) may have difficulties in conducting adequate multi-stakeholder dialogues that intend to develop an appropriate privacy regulation. Thus, we suggest that an independent organization (c) should organize such a dialogue.

(a) In the past, multi-stakeholder dialogues have been often organized and moderated by nation states. Social security programs or environmental protection laws are just two examples that illustrate how national governments may successfully organize and moderate dialogues between various agents with different interests. However, multi-stakeholder dialogues for solving the challenges of big data have two limitations when organized by nation states. First, the risks associated with big data are not just a local issue, but a global challenge. Many states would have to cooperate

to ensure success of any framework agreement. It is quite possible that some states would attempt to implement (transnationally) the results of stakeholder dialogues from their jurisdictions. Neither of these two possibilities seem practicable in the near future. Second, if only some states organize and moderate multi-stakeholder dialogues, the participants may accept standards that might cause adverse effects for the non-participants. This "beggar-my-neighbor" strategy would not result in an acceptable global standard because adversely affected parties have legitimate reasons to refuse participation.

(b) Scholars point out that firms can also conduct multi-stakeholder dialogues for regulatory frameworks (Pies et al., 2009, Scherer and Palazzo, 2007). In practice, many firms organize multi-stakeholder dialogues for developing further their corporate strategies or for gaining legitimacy for their business models (Palazzo and Scherer, 2006). Of course, companies can organize multi-stakeholder dialogues for their individual challenges considering big data. However, corporate stakeholder dialogues may not be applicable to or may be inappropriate for the challenges of big data, which affects the global economy and is not only a problem of a special industry.

(c) The (potential) shortcomings of governmental and corporate multi-stakeholder dialogues call for an independent organization that is able to undertake well-governed, international meetings. The challenge is to design an independent organization that is accountable and open to private, corporate, scientific and governmental interests in a democratic way and be able to develop and govern appropriate solutions for protecting privacy on a global scale in the age of big data. This is an extreme challenge: to balance complex and often conflicting stakeholders' interests with the need for appropriate privacy standards. The design of such an organization is discussed in the following sub-sections.

(2) *The organizational design for an appropriate multi-stakeholder dialogue*: An independent and credible organization that is able to conduct the necessary multi-stakeholder dialogues has to consider the process and the output dimension of the dialogue:

(a) *Process Dimension*: Baird's (2002) claim for accountable and open dialogues implies an important democratic principle. Affected stakeholders should have the opportunity to express their personal interests within the dialogues. However, because of the global dimension, it would be nearly impossible to implement a process that gives voice to everyone who might be affected. From a practical perspective, the participating parties should represent different stakeholder groups who represent the various interests (for example representatives of users, scientists, corporations, governments, etc.). Accountability is another important factor of the process dimension. The interested public should have the opportunity to verify that representatives actually represent them. The dialogue framework should also require a guideline to handle parties that deliberately interrupt the discourse for their own ends.

(b) *Output dimension*: Accountability and openness are important but not sufficient process criteria to ensure legitimacy for the multi-stakeholder dialogue and the conducting organization. The global scale of the dialogue and the various stakeholders' interests additionally require output criteria for gaining legitimacy. Homann (1988) and Hielscher et al. (2014) argue that a necessary criterion for legitimacy, in this context, is that the stakeholders accept the dialogue's results.

Even the best-governed dialogue (which is the process dimension) will not necessarily result in a privacy regulation that is fully accepted by all affected parties. Thus, the legitimacy – and the acceptance – of the discourse also depend on the output of the multi-stakeholder dialogue (Hielscher et al., 2014, Scharpff, 1999). This condition for gaining legitimacy and acceptance brings up a complex issue: is it really necessary that stakeholders fully accept every single part of a potential regulatory framework? Of course not: the decisive criterion is a regulatory framework that leads to a mutual betterment of every stakeholder compared to the status quo. A potential regulatory framework, from a practical standpoint, may probably include some rules that are not welcome to some parties. But this is not a decisive criterion; it is the potential of the whole framework that makes the difference. Otherwise, the scope for an appropriate and applicable privacy regulation would be tremendously limited.

Following the conceptual perspectives of Buchanan and Tullock (1962), Buchanan (2000) as well as Brennan and Buchanan (1985) for evaluating constitutional changes, it would be in the best interests of all stakeholders if they (only) compare the relevant alternatives of regulatory reforms with the status quo without also considering utopian ideas. This would free the discourse from idealistic but unworkable changes. This is an output-orientated process of small, but mutually beneficial steps, continuously improving the regulation. On the one hand, this process will hardly lead to a "great" solution that might be implemented immediately. On the other hand, stakeholders do not have to discuss hyper-theoretical reforms without exactly knowing the consequences. Instead, they can discuss changes by knowing the immediate consequences of these changes.

Hielscher et al. (2014) emphasize that an output oriented perspective that focuses on mutual gains compared to the status quo is also open for a so-called hypothetical consensus (Buchanan, 2000, p. 213). A regulatory framework might be legitimate as long as affected parties "could *in principle* either agree to the status quo or to an institutional reform of the status quo" (Hielscher et al., 2014, p. 539). This does not preclude affected parties being asked about their consensus. This also facilitates multi-national stakeholder dialogues in an appropriate way because dialogues would be impossible if every single opinion of a global society were to be considered.

To reach mutually acceptable solutions, we present the relevance of transaction costs, the enforceability of privacy and the issues of valuing private data for achieving social benefits or ills. Thus, a stakeholder dialogue can reach mutually acceptable solutions as long as the participants develop a regulatory framework that finds appropriate solutions for transferring property rights on private data, enforcing privacy rights and how to evaluate private data.

(3) *The implementation and governance of the dialogues' results*: We now discuss how this regulatory framework might implement and govern the results of the stakeholder dialogues.

The implementation of a privacy regulation that supports the development of big data in a responsible way has both a technical and an organizational dimension. First, companies, scientists, and also governments have to implement the regulatory framework in their data-collecting, data-processing, and data-sharing technologies. Besides the challenges of the technical implementation in current technologies, companies, scientists, and governments have the challenge of applying the regulation in their organizational processes. Existing business models have to be adapted or

existing routines of collecting, processing and sharing data have to be changed. Such changes may have an impact on the goals of the organization or the policies of government. Additionally, even a well-designed regulatory framework may not be acceptable to users because of the fear of exploitation through technologies or adverse organizational processes. Thus, to support the implementation, a credible commitment of companies, scientists and governments might be necessary so that these organizations implement the regulatory framework. The following approaches could contribute to a functional commitment of the actors that work with private data.

(a) *Certification for signaling*: Companies, scientists and governments that implement the regulatory framework would receive a certificate that indicates that they have implemented and are following the privacy regulation. This would tend to create an atmosphere of trust that would be beneficial to those who collect, process, and share data.

(b) *Fines for sanctioning*: Offences against the regulation by companies, scientists and governments could be punished, e.g., through a withdrawal of the certificate causing a loss of reputation. Fearing this, these participants may bind themselves to the regulation. The fear of reputation losses may not be sufficient for disciplining some participant's behavior. In this case, a fine for violations is also levied. In this setting, companies, scientists and governments would only receive a certificate if they agreed to accept fines in the case of violations.

(c) *Whistle blowing for revealing violators*: Finally, binding mechanisms are only functional for developing credibility and legitimacy of the privacy regulation if violations are recognized. However, violations of privacy, in many cases, create so called "victimless" crimes because the victims do not realize that they are a victim of a privacy violation. Consequently many privacy violations remain undetected and, thus, violators are not sanctioned. Needless to say, this would negatively influence the credibility and legitimacy of the privacy regulation.

However, measures exist that can handle this issue. Corruption and insider trading also create "victimless" crimes (Pies and Sass, 2006, Pies, 2008, Pies and Beckmann, 2009, Will and Pies, 2014). Even prosecuting authorities fail to prosecute this crime with traditional measures because "victimless" crimes cause a situation in which the authorities do not have a reasonable suspicion. In these cases, whistle blower legislation that protects the anonymity of the confidants can lead to evidence for reasonable suspicion coming to light. In the cases of corruption and insider trading, whistle blowing is appropriate because the reasonable suspicion leads to investigators checking account activities and asset acquisitions: the whistle blower's suspicions can be quickly checked. In these situations, lengthy proceedings that may victimize wrongfully accused people are rare.

In the case of privacy violations through big data applications, codes or log files may exist that indicate an abuse. A whistle blowing mechanism might be necessary to ensure that violations can be sanctioned. Against this backdrop, the next section presents the design of a privacy organization that might be able to organize and govern the implementation of an appropriate stakeholder dialogue.

4. Implications: Designing a Privacy Organization for an Appropriate Regulation in the Age of *Big Data*

Figure 2 illustrates how a privacy organization may be designed (1) to conduct multi-stakeholder dialogues and (2) to supervise the implementation of the dialogue's results.

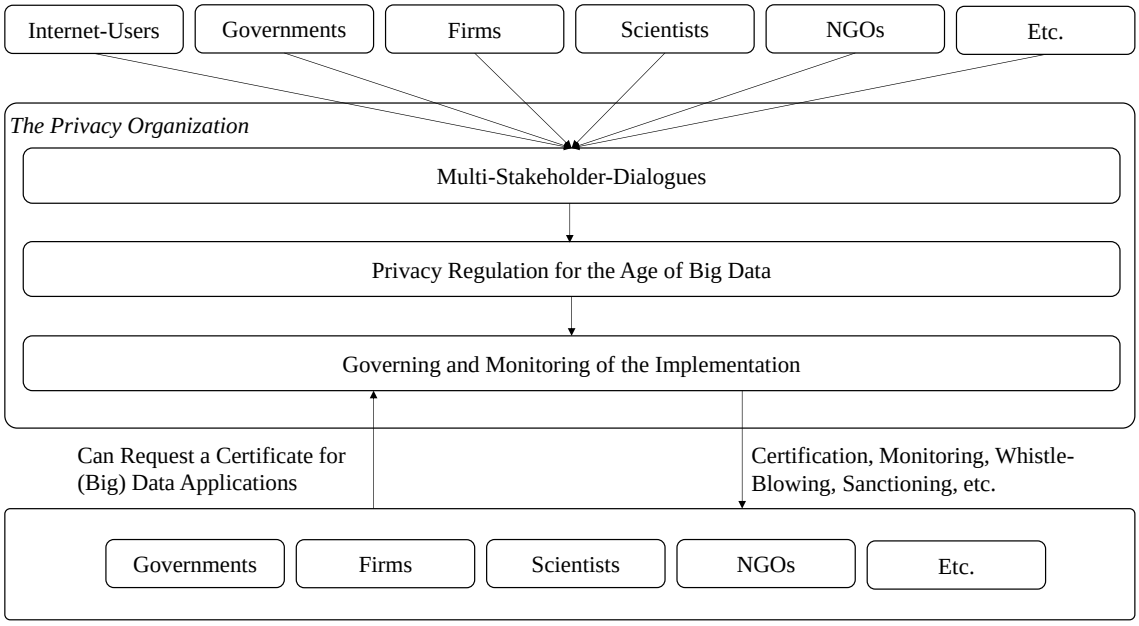

Figure 2: The potential design of a privacy regulation for developing and implementing an appropriate regulation of big data (own illustration)

(1) Conducting *multi-national stakeholder dialogues*: The privacy organization is responsible for the multi-stakeholder dialogue. It invites representatives of different stakeholder groups and sets an agenda for the discursive process that is in line with the interests of the stakeholders. Considering the current regulation of privacy and big data, the stakeholder dialogue may be focused on developing an "International Bill of Digital Rights" (Change.org, 2015). This framework defines fundamental rights and duties of users, companies, scientists and also governments. Therefore, the privacy organization initiates a stakeholder dialogue and governs this process, and moderates it in such a way that the stakeholders can reach a framework solution that generates mutual benefits compared to the status quo. Therefore, the framework should explicitly consider in the substantive part that a reduction of transaction costs, the enforceability of privacy and the value of private data are highly relevant factors for gaining mutual benefits through big data applications.

After establishing a general framework (e. g., an "International Bill of Digital Rights"), more detailed rules (e. g., a code of conduct for companies) can be established in a second step through additional dialogues. The privacy organization also considers the process and output dimension to achieve results acceptable to all. In this process, the privacy organization also ensures that the more detailed rules do not contradict the more general rules. Dialogues for reaching more detailed rules can be delegated to more specialized sub-groups. This may facilitate the whole dialogue for a comprehensive regulatory framework of privacy.

Reaching a legitimate dialogue acceptable to all may require a self-binding of the privacy organization, e.g., with a statute that expressly clarifies this point. This statute should underline the need for accountable and open processes, the focus of which is to create a regulation that leads to mutual benefits for the stakeholders. In addition, this organization needs a sufficient endowment capital for employing independent

people that can develop, support and govern this process.

(2) *Implementing and supervising the results*: The privacy organization may also be responsible for supervising the implementation of the privacy regulation by certifying companies, governments and scientific organizations. These organizations are then allowed to use the certificate as a label for signaling users that they handle private data responsibly. If users or whistle blowers inform the privacy organization about potential offences, the privacy organization has the right to investigate according to its statute. In case of a violation, the privacy organization can impose sanctions against the offending company, government or scientific organization. This can include fines against the violating organization and its employees who defy the privacy regulation. The privacy organization can also revoke the certificate. The privacy organization conducts these measures by following general principles of the rule of law. These principles act as a general authorization for potential sanctions, which might be part of the "Bill of Rights for the Digital Age". Additional norms can specify these general rules. The multi-national stakeholder dialogue (or the sub-dialogues) may develop adequate principles and norms for supervising and sanctioning.

Final Remarks and Discussion

To begin with, (1) we maintain that the discourse about whether private data are private or part of a (global) commons is misleading as is also the question (2) whether we need either a governmental regulation or a (corporate) self-regulation. (3) We highlight the fact that the idea of an international privacy organization has some precedents in the field of (international) technology standards. (4) A regulatory framework for the mutual interests of all parties in a well-governed internet gives functional incentives for companies to resolve privacy issues by themselves in a socially desirable way. (5) A regulatory framework (and the privacy organization) should be aware that corporations are only one actor that might abuse privacy – governments may be another. (6) Finally, we will argue that an adequate regulatory framework can only be based on a stakeholder dialogue because of its complexity. Against this backdrop, we present some questions that might guide the stakeholder discourse in a constructive direction.

(1) *Privacy or commons*: There is a broad discussion about whether private data should be private or a common resource in the internet age (Rifkin, 2014, pp. 75-77). In this debate, it makes little sense to discuss whether data are private or part of the commons a priori, if we are attempting to find a constructive solution to the privacy question. This question cannot be solely answered by the positive nature of data. Moreover, we have to ask what do we want as individuals and as society? Answering this question depends on the social effects that emerge if we define private data as private or as a common resource. Thus, a more constructive question might be to ask: what would a regulatory framework look like that is more beneficial for the immediately affected parties and society as a whole? Two perspectives are very relevant here: (a) static and (b) dynamic.

(a) A static perspective would allow one to concentrate on the direct effects of a concrete regulatory framework: who benefits and who loses in the short term? For example, how are individuals and organizations affected if private data became part

of the commons? Such a socialization of the available private data (in a new regulatory regime) might even have more benefits than losses because everyone could benefit from this common resource (Rifkin, 2014, pp. 75-77).

(b) However, by evaluating only the short-term social effects of regulatory changes, this static analysis may mislead us because the longer term consequences are also important. For example, a socialization of private data could encourage users to develop avoidance strategies to protect their data with consequent loss of benefit to society because the availability of new data is going to decline significantly.

Examination of the static and dynamic effects of regulatory reforms involves an evaluation of the behavioral effects that emerge immediately and indirectly. Some factors that may influence this evaluation include: the level of privacy that we concede as a society depends on the stakeholders' needs, the technology (for example, big data applications, data safety, etc.) and governance (e.g., enforceability of privacy, transaction costs emerging when we want to transfer data, etc.). The complex interdependencies between these determinants call for a well-designed regulatory framework that defines which data are private and which are part of the commons. Therefore, we see stakeholder discourses as essential means to deal with the various stakeholders' needs and technological constraints. In addition, the technological and social developments may call for regular dialogues for improving the framework.

(2) *Regulation by governments or self-regulation*: Some scholars debate the extent to which the internet and privacy should be governed by governments or self-regulation (Weber, 2010, Schwartz, 2000, Goldsmith, 1997-1998). On the one hand, national governments can develop and implement a regulatory framework that might work in their jurisdiction. In addition, national governments can cooperate with other nations or initiate multi-stakeholder dialogues on a national or multi-national level. Of course, a national or multi-national regulation only works in the participating jurisdictions. On the other hand, users, companies and civil society organizations may organize a self-regulation of the internet. However, this requires organizations that guide and govern the implementation of regulatory initiatives. The privacy organization discussed above may be the first step for such a self-regulatory process that is independent of the source of the initiative – either from government or the internet community.

Legitimacy and acceptance of regulation are considered very relevant aspects of this process. Regulatory initiatives by democratic states can build on the legitimacy of their democratic processes. However, the regulatory initiatives of big (democratic) states may cause path dependencies in smaller countries. For example, the understanding of privacy in the U.S is different from that of many European states. International US companies have to follow US privacy law. This often causes conflicts in European states (where these companies operate) because European users have different demands regarding their privacy. Thus, internet users in one country do not have to accept a regulatory framework that is legal in another (democratic) country.

A potential self-regulation does not have to result in a legitimate framework. If powerful lobby groups exploit self-regulatory processes, self-regulation is not possible. Therefore, the multi-stakeholder dialogue presented here calls for an accountable and open process for increasing legitimacy. Finally, the output

dimension is another relevant criterion to gain legitimacy. The second section presents three substantial criteria for achieving this: transferability of property rights on private data, enforceability of privacy rights and considering the value of private data.

(3) *Precursors of an international privacy organization*: In the field of technology and standardization, several organizations exist that deal with similar issues like an international privacy organization. A well-known example is the International Organization for Standardization (ISO) which establishes international proprietary, industrial and commercial standards through multi-stakeholder dialogues. Two other relevant organizations are the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU). These organizations can be a blueprint for an international privacy organization regarding funding, legal status, the organization of multi-national stakeholder dialogues and the implementation of the results.

(4) *The relevance of a well-designed privacy framework for companies*: A well-designed privacy framework is not only in the interest of users, it is also relevant for the business sector. Companies do not have to fear (a) that competitors may use data illegally for increasing their market power or (b) losses of reputation through privacy scandals because of rogue firms in the same industry. An international privacy organization that implements privacy standards may also prevent regulation for the sake of regulation by national politicians. In addition, international companies can base their business models on international standards and do not have to adapt their businesses according do different national standards.

Moreover, a well-designed regulatory framework gives important stimuli for inventions that solve social issues. So far, companies that use big data applications operate in a twilight zone that results in many implicit costs: e.g., companies may avoid beneficial big data applications because of fearing bad news and unjustified accusations by civil society organizations. This reduction of innovation due to self-censorship may be reinforced by users not disclosing private information. In a mutually beneficial paradigm, companies would benefit through new business models and society would also benefit because of new solutions for unresolved issues.

From this perspective, users and companies ought not to be in conflict but instead have mutual interests in a well-designed regulatory framework. Companies acting as good corporate citizens will initiate and support multi-stakeholder dialogues because it is in their genuine self-interest. Thus, being a corporate citizen does not conflict with long-term business models.

(5) *Abusers of privacy*: Many users consider companies to be privacy violators. Whereas this may be true, governments are also interested in private data. Even in democratic countries, politicians and bureaucrats may neglect basic privacy standards. In addition, private companies may be forced to cooperate with governments. This holds for undemocratic countries and also democratic nations as the NSA scandal reveals (Ball et al., 2013, Goede, 2014, Hahn et al., 2015, Perlroth et al., 2013). These deficiencies are a problem for users and also a risk for companies. If violations through governments become public, companies might be the recipient of criticism because companies have “co-operated” with governments. Another consequence may be that prejudices against big data emerge resulting in a general

criticism against all, even responsible big data applications. A global privacy organization that has open and accountable standards may also bind governments not to abuse their power. In addition, it may also bind companies to refuse illegal or illegitimate inquiries by governments because of a greater fear of privileges for co-operating competitors or dreadful lawsuits.

(6) *Dealing with complexity*: The design of a regulatory framework for privacy in the internet age has to contend with at least three fields of complexity: (a) technology, (b) pluralism, (c) network externalities.

(a) First, technology and continuing innovations require a framework that is adaptable to different technological solutions and even to applications that have not yet been developed. In addition, the implementation of a regulatory framework may be difficult because the incredible number of lines of code make security gaps likely. Thus, the development of a regulatory framework and its implementation is likely to be long-lasting considering its own deficiencies and technological developments.

(b) Second, a regulatory framework that governs the World Wide Web has to find solutions for the complex problems of a pluralistic (world) society. People have various understandings of privacy and may accept different interventions in their privacy through private firms and governments. Thus, a regulatory framework has to be superior to the status quo to get broadly accepted. We are sure that a framework can exist that treats fairly the pluralistic interests of users, companies, governments and scientists. The processes for developing and implementing this framework must be open (in principle), accountable and consider the above discussed output dimension for broad acceptance.

(c) Finally, the network externalities that can emerge through big data applications are another obstacle for developing an acceptable privacy regulation. In a world without transaction costs, everyone would be better off if we would internalize positive effects that emerge through big data applications (Coase, 1960, Demsetz, 1967,). This means that users would be compensated directly in the amount of the benefits that companies generate through these applications. As argued in the second section, transaction costs may prevent a "fair" compensation or even lead to a situation in which a "fair" compensation has more disadvantages than benefits. Thus, we have to find other criteria for increasing users' acceptance for big data applications.

One criterion for acceptance might be that companies or governments do not exploit users. In this setting, users would trust companies and governments that their private data is handled with care. However, because of the positive externalities, trust alone may not be sufficient because users want to benefit if they provide private data.

The general system logic of the internet may satisfy the desire for a "fair" compensation. Access to the internet is more or less open and users can benefit from the many services that are the result of big data applications (e.g., powerful search engines) or go hand in hand with big data applications (e.g., applications that are co-financed by so-called two-sided markets like online newspapers). At the same time, the competition between internet firms creates more and more services that increase the users' willingness to share private data because the services are so attractive. Thus, competition among firms may be the best guarantor of a redistribution of big data rents to the users. The redistribution process is not necessarily only monetary because users can benefit from new and cheap applications. Of course, this process

may result in that not every positive network externality can be redistributed to the users because of low competition in narrow markets. In addition, some users may receive less benefits than others because of their consumptions behavior in the internet. But this should not be a decisive criterion for evaluating the users' gains that emerge through big data applications in general – because in a well-governed internet, the internet will generate so many benefits for the users as long as they desire these gains.

Finally, all these challenges depend on the question how we govern big data and privacy. This paper presents some procedural and substantive suggestions for designing an appropriate regulation in the age of big data.

Literature

Adderley, Richard (2004): The Use of Data Mining Techniques in Operational Crime Fighting, in: Intelligence and Security Informatics, Second Symposium on Intelligence and Security Informatics, ISI 2004, Tucson, AZ, USA, June 10-11, 2004, Proceedings, Springer, Berlin, pp. 418-425.

Baird, Zoe (2002): Governing the Internet: Engaging Government, Business, and Nonprofits, in: Foreign Affairs, Vol. 81, No. 6, pp. 15-20.

Ball, James, Julian Borger and Glenn Greenwald (2013): Revealed: How US and UK spy agencies defeat internet privacy and security, in: The Guardian, Thursday 5 September 2013, download via http://www.ihatefeds.com/Revealed_%20How%20US%20and%20UK%20spy%20agencies%20defeat%20internet%20privacy%20and%20security%20_%20World%20news%20_%20The%20Guardian.pdf, 02.07.2015.

Boyd, Danah, and Kate Crawford (2012): Critical Questions for Big Data, in: Information, Communication & Society, Vol. 15, No. 5, pp. 662-679.

Brennan, Geoffrey, and Buchanan, James M. (1985): The Reason of Rules: Constitutional Political Economy, Cambridge University Press, London.

Buchanan, James M. (2000): The Limits of Liberty: Between Anarchy and Leviathan, The Collected Works of James M. Buchanan, Liberty Fund, Indianapolis.

Buchanan, James M., and Gurdon Tullock (1962): The Calculus of Consent: Logical Foundations of Constitutional Democracy, University of Michigan Press, Ann Arbor.

Change.org (2015): A Stand for Democracy in the Digital Age, https://www.change.org/p/a-stand-for-democracy-in-the-digital-age-3, 11.06.2015.

Chen, Hsinchun, Roger H. L. Chiang, and Veda C. Storey (2012): Business Intelligence and Analytics: From Big Data to Big Impact, in: MIS Quarterly, Vol. 36, No. 4, pp. 1165-1188.

Coase, Ronald H. (1960): The Problem of Social Cost, in: Journal of Law and Economics, Vol. 3, pp. 1-44.

Davenport, Thomas H., Paul Barth and Randy Bean: How 'Big Data' Is Different, in: MIT Sloan Management Review, Vol. 54, No. 1, pp. 22-24.

Demsetz, Harold (1967): Towards a Theory of Property Rights, in: The American Economic Review, Vol. 57, No. 2, pp. 347-359.

Goede, Marieke de (2014): The Politics of Privacy in the Age of Preemptive Security, in: International Political Sociology, Vol. 8, pp. 100-118.

Goldsmith, Jack (1997-1998): Regulation of the Internet: Three Persistent Fallacies, in: Chicago-Kent Law Review, Vol. 73, pp. 1119-1131.

Hahn, Tobias, Paul C. Johannes and Benjamin Lange (2015): Schutzschilde gegen die NSA – Wie Deutschland seine Bürger durch Anleitung zur Selbsthilfe vor Internetspionage schützen muss, in: Datenschutz und Datensicherheit, Vol. 2-2015, pp. 71-77.

Hielscher, Stefan, Markus Beckmann and Ingo Pies (2014): Participation versus Consent: Should Corporations Be Run according to Democratic Principles?, in: Business Ethics Quarterly, Vol. 24, No. 4, pp. 533-563.

Hill, Richard (2014): The Internet, Its Governance, and the Mulit-Stakeholder Model, in: Info, Vol. 16, No. 2, pp. 16-46.

Homann, Karl (1985): Legitimation und Verfassungsstaat, in: Jahrbuch für Neue Politische Ökonomie, Vol. 4, pp. 48-72.

Homann, Karl (1988): Rationalität und Demokratie, Mohr Siebeck, Tübingen.

Iansiti, Marco, and Karim R. Lakhani (2014): Digital Ubiquity: How Connections, Sensors, and Data Are Revolutionizing Business, in: Harvard Business Review, November 2014, pp. 91-99.

LaValle, Steve, Eric Lesser, Rebecca Shockley, Michael S. Hopkins and Nina Kruschwitz (2011): Big Data, Analytics and the Path from Insights to Value, in: MIT Sloan Management Review, Vol. 52, No. 2, pp. 21-31.

McAfee, Andrew, and Erik Brynjolfsson (2012): Big Data: The Management Revolution, in Harvard Business Review, October 2012, Reprint.

Palazzo, Guido, and Andreas Georg Scherer (2006): Corporate Legitimacy as Deliberation: A Communicative Framework, in: Journal of Business Ethics, Vol. 66, pp. 71–88.

Pentland, Alex (2014): With Big Data Comes Big Responsibility – An Interview with MIT Media Lab's Alex "Sandy" Pentland, in: Harvard Business Review, November 2014, pp. 101-104.

Perlroth, Nicole, Jeff Larson and Scott Shane (2013): N.S.A. Able to Foil Basic Safeguards of Privacy on Web, in: The New York Times, September 5, 2013, download: http://ctvoterscount.org/CTVCdata/13/09/NYTimes20130905.pdf, 02.07.2015.

Pies, Ingo (2008): Wie bekämpft man Korruption?, Wissenschaftlicher Verlag, Berlin.

Pies, Ingo (2009): Gier und Größenwahn? – Zur Wirtschaftsethik der Wirtschaftskrise, Discussion Paper No. 2009-18 of the Chair in Economic Ethics, Martin-Luther-University Halle-Wittenberg, edited by Ingo Pies.

Pies, Ingo (2012): Terminmarktgeschäfte erfüllen eine wichtige Versicherungsfunktion: Ein Interview zur Finanzspekulation mit Agrarrohstoffen, Discussion Paper No. 2012-28 of the Chair in Economic Ethics, Martin-Luther-University Halle-Wittenberg, edited by Ingo Pies.

Pies, Ingo, Markus Beckmann and Stefan Hielscher (2014): The Political Role of the Business Firm: An Ordonomic Re-Conceptualization of an Aristotelian Idea, in: Business & Society, Vol. 53, No. 2, pp. 226–259.

Pies, Ingo, und Markus Beckmann (2009): Whistle-Blowing heißt nicht: "verpfeifen" – Ordonomische Überlegungen zur Korruptionsprävention durch und in Unternehmen, Discussion Paper No. 2009-19 of the Chair in Economic Ethics, Martin-Luther-University Halle-Wittenberg, Halle.

Pies, Ingo, und Peter Sass (2006): Korruptionsprävention als Ordnungsproblem – Wirtschaftsethische Perspektiven für Corporate Citizenship als Integritätsmanagement, in: ORDO, Vol. 57, pp. 341-369.

Rifkin, Jeremy (2014): The Zero Marginal Cost Society: The Internet of Things, The Collaborative Commons, and the Eclipse of Capitalism, Palgrave Macmillian, New York.

Scharpff, Fritz W. (1999): Governing in Europe: Effective and Democratic?, Oxford University Press, New York.

Scherer, Andreas Georg, and Guido Palazzo (2007): Toward a Political Conception of Corporate Responsibility: Business and Society Seen from a Habermasian Perspective, in: Academy of Management Review, Vol. 32, No. 4, pp. 1096–1120.

Schwarz, Paul M. (2000): Internet Privacy and the State, in: Connecticut Law Review, Vol. 32, pp. 815-859.

Solove, Daniel J. (2008): Understanding Privacy, Harvard University Press, Cambridge.

Tene, Omer, and Jules Polonetksy (2012). Privacy in the Age of Big Data: A Time of Big Decisions, in: Stanford Law Review Online, Vol. 64:63, pp. 63-69.

Tene, Omer, and Jules Polonetksy (2013): Big Data for All: Privacy and User Control in the Age of Analytics, Vol. 11, No. 5, pp. 239-273.

Welber, Rolf H. (2010): Internet of Things – New Security and Privacy Challenges, in: Computer Law & Security Review, Vol. 26, pp. 23-30.

Will, Matthias Georg, and Ingo Pies (2014): Insiderhandel und die Neuorientierung der Kapitalmärkte: Ein Beitrag zur Regulierungsdebatte in Europa, in: ORDO, Vol. 65, pp. 159-181.

Diskussionspapiere[1]

Nr. 2015-3	**Matthias Georg Will** Privacy and Big Data: The Need for a Multi-Stakeholder Approach for Developing an Appropriate Privacy Regulation in the Age of Big Data
Nr. 2015-2	**Ingo Pies** Diskurs mit Schieflage Eine ordnungsethische Nachbetrachtung der Mindestlohndebatte
Nr. 2015-1	**Ingo Pies** Ordnungsethik für eine bessere Ordnungspolitik: Ordonomische Anregungen zum schulischen Bildungsauftrag
Nr. 2014-19	**Ingo Pies** Laudatio Max-Weber-Preis 2014 in der Kategorie Ausbildungs-Studienpreis
Nr. 2014-18	**Ingo Pies** Die Gerechtigkeitsdebatte in Deutschland: Diskursversagen beim Mindestlohn
Nr. 2014-17	**Ingo Pies** Der ordonomische Ansatz: eine Illustration am Beispiel des Mindestlohns
Nr. 2014-16	**Ingo Pies** Hunger durch Agrarspekulation?
Nr. 2014-15	**Ingo Pies** Führen mit Werten in Politik und Wirtschaft
Nr. 2014-14	**Ulrich Koester, Ingo Pies** Policy recommendations require more than just technical information. A comment
Nr. 2014-13	**Ingo Pies** Wirtschaftsethik der Welternährung
Nr. 2014-12	**Ingo Pies** F.A. von Hayek und die moralische Qualität des Wettbewerbs
Nr. 2014-11	**Ingo Pies** Argumentiert Papst Franziskus marktfeindlich? Wirtschaftsethische Stellungnahme zum Apostolischen Schreiben »Evangelii Gaudium«
Nr. 2014-10	**Ingo Pies** Interview zu CSR
Nr. 2014-9	**Ingo Pies** Nahrungsmittelspekulation: ein Interview
Nr. 2014-8	**Ingo Pies** Der Finanzsektor soll Hunger bekämpfen – Aber wie?
Nr. 2014-7	**Matthias Will, Ingo Pies** Insiderhandel und die Regulierung der Kapitalmärkte: Ein Beitrag zur MiFID-Debatte
Nr. 2014-6	**Ingo Pies** Interview zur Moral der Finanzspekulation mit Agrarrohstoffen und zur Ordnungsethik der Zivilgesellschaft
Nr. 2014-5	**Ingo Pies** Die Stunde der Symbolpolitik – Zur politischen Funktion wirtschaftlicher Zusammenarbeit in Krisenzeiten
Nr. 2014-4	**Ingo Pies, Oliver Holtemöller** Mit administrierten Löhnen Armut bekämpfen? – Warum die Debatte um den Mindestlohn in Deutschland verfehlt ist
Nr. 2014-3	**Ingo Pies. Stefan Hielscher** Miteinander oder Gegeneinander? – Zur Verhältnisbestimmung von Unternehmen und zivilgesellschaftlichen Organisationen
Nr. 2014-2	**Matthias Georg Will, Ingo Pies** Discourse and Regulation Failures: The Ambivalent Influence of NGOs on Political

[1] Free internet access at: http://ethik.wiwi.uni-halle.de/forschung

Nr. 2013-7	**Ingo Pies** Ethik der Agrarspekulation: Rückblick und Ausblick
Nr. 2013-6	**Ingo Pies** Agrarspekulation – Replik auf Hans-Heinrich Bass
Nr. 2013-5	**Ingo Pies** Agrarspekulation – Replik auf Thilo Bode
Nr. 2013-4	**Ingo Pies** Agrarspekulation? – Der eigentliche Skandal liegt woanders!
Nr. 2013-3	**Matthias Georg Will, Stefan Hielscher** How Do Companies Invest in Corporate Social Responsibility? An Ordonomic Contribution for Empirical CSR Research – A Revision
Nr. 2013-2	**Ingo Pies, Sören Prehn, Thomas Glauben, Matthias Georg Will** Kurzdarstellung Agrarspekulation
Nr. 2013-1	**Ingo Pies** Ordnungsethik der Zivilgesellschaft – Eine ordonomische Argumentationsskizze aus gegebenem Anlass

Wirtschaftsethik-Studien[2]

Nr. 2013-1	**Ingo Pies** Chancengerechtigkeit durch Ernährungssicherung – Zur Solidaritätsfunktion der Marktwirtschaft bei der Bekämpfung des weltweiten Hungers
Nr. 2010-1	**Ingo Pies, Alexandra von Winning, Markus Sardison, Katrin Girlich** Sustainability in the Petroleum Industry: Theory and Practice of Voluntary Self-Commitments
Nr. 2009-1	**Ingo Pies, Alexandra von Winning, Markus Sardison, Katrin Girlich** Nachhaltigkeit in der Mineralölindustrie: Theorie und Praxis freiwilliger Selbst-verpflichtungen
Nr. 2007-1	**Markus Beckmann** Corporate Social Responsibility und Corporate Citizenship
Nr. 2005-3	**Ingo Pies, Peter Sass, Roland Frank** Anforderungen an eine Politik der Nachhaltigkeit – eine wirtschaftsethische Studie zur europäischen Abfallpolitik
Nr. 2005-2	**Ingo Pies, Peter Sass, Henry Meyer zu Schwabedissen** Prävention von Wirtschaftskriminalität: Zur Theorie und Praxis der Korruptionsbekämpfung
Nr. 2005-1	**Valerie Schuster** Corporate Citizenship und die UN Millennium Development Goals: Ein unternehmerischer Lernprozess am Beispiel Brasiliens
Nr. 2004-1	**Johanna Brinkmann** Corporate Citizenship und Public-Private Partnerships: Zum Potential der Kooperation zwischen Privatwirtschaft, Entwicklungszusammenarbeit und Zivilgesellschaft

[2] Als kostenloser Download unter http://ethik.wiwi.uni-halle.de/forschung.