D. Hühnlein, H. Roßnagel, C. Schunck, M. Talamo (Eds.): Open Identity Summit 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 105

Non-technical Challenges of Building Ecosystems for Trustable Smart Assistants in the Internet of Things: A Socioeconomic and Legal Perspective

Michael Kubach[1], Caterina Görwitz[1], and Gerrit Hornung[2]

Abstract: In this position paper, we present non-technical challenges that arise while building ecosystems for trustable smart assistants in the Internet of Things. Such non-technical challenges are often neglected in the development process of information systems, even though they are important elements for their success. Only if the assistants are technically effective and fit into the non-technical framework conditions of their application area (e.g. the market structure, stakeholder, liability, and data-protection requirements), they will be able to become successful innovations. We will support this argument in our position paper, focusing on the socioeconomic and legal perspective.

Keywords: internet of things, smart assistants, smart services, ecosystems, socioeconomic perspective, legal perspective, data protection, business models, stakeholders, research project

1 Introduction

The present development in the context of the Internet of Things enables a new kind of smart services and smart assistants that support every user individually depending on his or her needs. Nevertheless, there are still some challenges on the way that need to be overcome.

Many of the challenges found in building smart assistants are rather technical and refer to aspects like interoperability or IT security. However, smart assistants require the combination of various data from several sources and therefore the cooperation of various stakeholders. Moreover, people will only be willing to use the assistants in their daily lives if they trust them and if they comply with the rules that govern these lives. These are all non-technical aspects and in this position paper, we are going to put our focus on them, as practical experience from the history of information systems has shown that they have often been overlooked.[3] Examples to how problematic an insufficient consideration of these factors can be for the long term success of modern IT solutions can be illustrated with two relatively new German projects; DE-Mail and the new German elec-

[1] Fraunhofer IAO, Nobelstr. 12, 70569 Stuttgart, vorname.nachnname@iao.fraunhofer.de
[2] Universität Kassel, Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht, Kurt-Schumacher-Str. 25, 34117 Kassel, gerrit.hornung@uni-kassel.de
[3] There is, however, related work from other research projects that we can build on. Such is the EU FP7 Project "SmartSociety" that has produced insights on ethical aspects for hybrid systems where people and machines tightly work together to build a smarter society (www.smart-society-project.eu).

tronic identity card (neuer Personalausweis or "nPA"). In spite of high technical effectiveness and security, both solutions fail to succeed in the market. Therefore, a prime aim of this paper will be to address particularly the socioeconomic and legal challenges in building ecosystems for trustable smart assistants in the Internet of Things. In addition to the latter, technical challenges will be thoroughly investigated in a new research project, which is briefly presented later in the paper. We expect that the discussion and feedback on our position paper can be of high value for the future course of this research project.

The remainder of this paper is structured as follows. In the second chapter, we clarify some basic terms in the relatively young field of trustable smart assistants and ecosystems in the Internet of Things. The third chapter then focuses on the socioeconomic challenges and issues that may emerge from smart assistants in the Internet of Things to a success on the market. The fourth chapter specifies legal issues that appear on different stages of the work of smart assistants, namely: personal data protection and processing, data collection, the principles of transparency and data minimization, and liability. Moreover, it draws links to the new EU General Data Protection Regulation. The fifth chapter then presents the ENTOURAGE research project – an open ecosystem for smart assistants – that will address the challenges stated in the previous chapters in the next three years of its development. Finally, the paper finishes with a short conclusion.

2 Ecosystems for Trustable Smart Assistants in the Internet of Things

2.1 Trustable Smart Assistants

Assistance systems store, process, and transmit information and support users in personal decisions in a variety of life situations. Nevertheless, these assistants cannot be reduced to technology alone. An essential factor is the interaction with the user and the reaction to a certain context. Therefore, in general, assistance systems are contextual and personalized [GM02].

In the last years, there has been an increasing interest in the development of intelligent personal assistants in research and practice. Some voice-controlled products such as Apple's Siri, Google's Now, Microsoft's Cortana or Amazon Echo are already in the market. Some studies have been researching the trustworthiness and acceptance of such systems. Moorthy and Vu [MV14] have analyzed the acceptance of personal assistants that are integrated in smartphones. The results show that the willingness to deliver private information via the natural language interface depends on the particular location and context of the user. Glass et al. [GMW08] have identified some factors, which are important for the trust of users towards personal assistants. The systems should be designed transparent, so that it is evident for the user to understand which steps are carried out for what reasons. Moreover, the user should be able to find out the sources where the system

finds the requested information. Finally, personal assistants should not be designed too autonomously, so that the users always have the power to change or adjust the functions and consequences induced.

Nevertheless, it should be noted that not only end-users are required to trust the assistants. Other stakeholders in the ecosystem (see next section) should also be able to trust in the fact that, for example, the data of their sensors are not misused and they are compensated appropriately for the services they provide. Moreover, if wrong decisions have been made, liability questions could become an issue. So far, these aspects of trust have hardly been considered in the literature.

2.2 Ecosystems for Smart Assistants

To date, existing smart assistants are limited to a large extent to the IoT platforms of their vendors or operators. A platform is considered to be a set of technological building blocks and complementary assets that companies, entrepreneurs and individuals can use and consume to develop complementary products, technologies and services [Mu13]. The restriction to single "platform-silos" significantly hinders the combination of application fields and cross-platform use of data and thus the achievement of the full potential of smart services.

This is why an open ecosystem for smart assistants is that valuable. Following Muegge [Mu13], the ecosystem-approach towards smart assistants is much broader than the platform-approach. It overcomes some of its limitations and further extends it towards the (economic) actors involved. In the networked ecosystem of interdependent and codependent actors with partially aligned incentives, a technology entrepreneur can achieve more, learn faster, and reach farther than otherwise possible, while sharing some of the risks and costs with others. The ecosystem is not defined and limited to one single (technological) platform, but rather through the outcome and incentives that are more or less shared among the different actors in the ecosystem.

By constructing such an ecosystem, it will become possible for the assistants to filter data from different sources, aggregate it, process it and make it easily accessible to the users. Additionally, user interfaces could be made available at higher levels, or even autonomous decisions within the framework of determined users' preferences taken. Therefore, such assistants as intelligent smart services in respective open ecosystems represent a key technology for the development of the potential of the Internet of Things.

3 Socioeconomic Challenges

The current separation of platforms for smart assistants follows economic interests. The manufacturers of smart end devices have invested resources for development and operation of these devices in order to finally obtain valuable sensor data. There is no function-

ing mechanism that allows for flexible integration of new actors and their information, services or devices into this system, and takes into consideration the particular economic interests.

A crucial challenge is to analyze how such an ecosystem can be offered and used in an economically viable form. Particularly in an open ecosystem, where different actors deliver and use data and offer services based on that data (in this case particularly to assistants), the consideration of incentive and pricing models is necessary. Otherwise, this exchange can hardly be reached. To achieve this, the economic framework conditions need to be appropriately analyzed and respective requirements for the components of the ecosystem need to be derived.

Powerful smart assistants in an ecosystem rely on an exchange of data and services between different actors. This exchange could be regarded as a type of a multi-sided market between data providers, operators of smart assistants, and end users. In addition, other actors like providers of specific services (e.g. big data analysts, platform operators, and vendors of technical devices) could also participate in this market. Analyzing the structure of this market and its participants will be the first step in developing appropriate framework conditions in the ecosystem such as a market place for data. No matter who exactly the participants in the ecosystem are, it is rather certain that the ecosystem will face a multi-sided market. This implies that the success of the ecosystem will depend on the successful coordination of the demand of the distinct actors who need each other in some way [Ev03]. Another aspect to consider is that the ecosystem is subject to network effects so that, for example, the attractiveness of the ecosystem increases for operators of smart assistants if more data providers are active. Furthermore, the ecosystem becomes more attractive for data providers and operators of smart assistants if more end users are able to use the smart assistants with their smartphones or from their cars. This can result in a positive feedback and thus in an exponential growth once a critical mass has been reached. However, this also works vice versa, resulting in a chicken-and-egg problem and negative feedback [MR99]. If there are no smart assistants in the ecosystem the incentives for data providers to offer their data in the format required for the ecosystem is presumably low. Therefore, when building the ecosystem the specific market-structure and respective strategies for entering the market as well as balancing the interests of its actors have to be considered.

As the previous section already indicated, identifying the incentive structures necessary for the acceptance of the ecosystem through its integral actors or stakeholders poses another important challenge. However, the analysis and the efficient management of multidiscipline requirements towards an ecosystem for smart assistants are not trivial. Therefore, currently discussed economic models and theories have to be evaluated for their applicability in the context of an ecosystem for smart assistants in the Internet of Things. One of these approaches is stakeholder theory with its practical application stakeholder analysis. Stakeholder analysis is an established socioeconomic method. It allows to specifically address the demands of the stakeholders of a certain organization, product, as well as technology and far exceeds a simple market analysis. In addition, it is

used successfully in the area of information systems [Po99]. Thus, a stakeholder analysis of the ecosystem seems to be necessary.

When the integral stakeholder and incentive structures are identified, viable business models for these structures can be developed. Only solutions developed in that way have the potential to meet market needs and technical performance requirements and later become successful [Ac14]. However, the development of viable business models is not a trivial process but pivotal to the success of new technologies. This is also represented in the discussions on business model approaches in Business Economics, Information Systems, and specifically literature on the Internet of Things [Ka15], [Li11], [EHB11], [ZA10], [OPT05].

The pricing strategy or a pricing model that is used in the business model is the final socioeconomic challenge that we want to highlight here. As we have shown, reaching the critical mass of actors in the ecosystem is crucial due to the multi-sided market and its network effects. Finding a suitable pricing strategy for the various actors is one important element in reaching the critical mass and sustaining the ecosystem. For other application areas with multi-sided markets various pricing strategies have been discussed in the literature, the main strategies being of a “divide-and-conquer” nature. In these strategies the participation of some actors on one side of the market (divide) is subsidized through revenues generated from the other side (conquer) [CJ03]. Of course, this depends on the willingness to pay of the actors as well, which has already been analyzed for multi-sided markets [Ro14] but not for the context of ecosystems smart assistants. Overall, this shows that pricing strategies are another important research gap and challenge building ecosystems for smart assistants.

4 Legal Issues

Smart assistants are assistants that know as much as possible about their owner. It is thus necessary to collect and exchange an ample amount of data. This can be considered critical because detailed behavioral, motion and personality profiles can be derived while working with smart assistants [ST05] [Gi07] or the Internet of Things in general [HH15a]. However, not all data in smart environments will be personal data that relates to an identified or identifiable person. Many smart objects and cyber-physical systems will produce “technical” data, which at first glance may look anonymous. One big challenge of the never-ending storage of this data could however be the long-term perspective, as the growing information in data bases might, in the end, lead to identifiable persons [Ro13].

To determine whether data is personal, Art. 2 (a) of the current Data Protection Directive defines an identifiable person as "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”. In its core activity, a trustable smart assistant in the Internet of Things will process a plethora of

data of this kind. This leads to the application of national data protection laws, as well as of the future General Data Protection Regulation (cf. below), because the latter will only slightly change the respective definition.

If the system is to process personal data, there has to be a proper legal basis for the processing, i.e. either legislation or an effective consent by the persons affected. Without such a legal basis, every collection and processing of personal data is illegal [SS14]. Hence there are two main options that allow data collection. On the one hand, data could be collected with the consent of the data subject according to Art. 7 (a) of the Data Protection Directive; on the other hand, a law that permits the collection is required [TF14]. For example, the collection could be used as a means for the performance of a contract according to Art. 7 (b) of the Data Protection Directive. These traditional mechanisms are highly debated nowadays, particularly as regards the question who may use personal data as a basis for new business models ("data ownership", cf. [HG15]).

If a legal basis has been found, the data controller must continue to comply with the principle of transparency. According to Art. 10 of the Data Protection Directive, the user of smart assistants must firstly be informed about the data controller, the purposes of the processing, and the recipients or categories of recipients to which these data are transmitted. This could be problematic if the data which is exchanged originate from different sources, as it may no longer be clear which controller currently stores the data and who is responsible for it. Moreover, the data collection and use should be as transparent as possible for the individuals concerned, especially when the data are transmitted and processed in "third countries" (i.e. outside the European Union and the European Economic Area). However, this transparency will be challenging due to the large number of participating data.

According to Art. 6 (1) (b) of the Data Protection Directive, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The original purposes may thus not be exceeded during the data processing. However, these purposes are hard to define in advance for smart assistants due to the increasing complexity of the surrounding ecosystem and the various targets of external stakeholders. Especially, when the purpose binding principle of Art. 6 (1) (b) of the Data Protection Directive is applied to very broad purposes it can lose its value [Ro13]. If the purpose of a smart assistant is defined as "to help the data subject in professional and personal settings in every respect, including situations and modes of assistance which are not yet clear", than literally every personal data may be regarded as being necessary to this end.

In addition, the principle of data minimization must be observed. Art. 6 (1) (c) of the Data Protection Directive indicates that as little personal information as possible should be collected. According to Art. 6 (1) (e) of the Data Protection Directive, this applies also to the duration of data retention, as the data has to be deleted or at least anonymized if the controller does not need it for the stated purpose anymore [Sc14]. This raises the question for how long the data may be stored, which becomes even more difficult to

answer if smart assistants use data to build a network that consists of these data and grows with them.

Another important point in question is the processing of special categories of personal data. Regarding to Art. 8 (1) of the Data Protection Directive, these kinds of data refer to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union memberships, and the processing of data concerning health or sex life. As smart assistants will collect data of many areas of personal life, it is very likely that this will include sensitive data of this kind. If smart assistants, for example, permanently track the current location of the user, this may include a stay in hospital, leading to the information about medical treatment. Data protection law then demands higher requirements: while a simple consent for normal personal data has to be "unambiguously given" in general, the consent for sensitive data must be "explicit" regarding these data. Depending on the number of consents and the technical design, this could be very burdensome.

Continuing, the guarantee of data security is another challenge. The more data a controller stores, the greater the interest from others will be to obtain access to this information. Especially cross-platform applications are very crucial as they increase the vulnerability for external attacks, because IT architectures will be designed more standardized and uniformly. As data security is not only a legal requirement (cf. Art. 17 of the Data Protection Directive), but also a prerequisite for any trust of the user in smart assistants, it will be mandatory for data controllers to ensure a high, state-of-the-art standard.

Further the question of liability must be addressed if shortcomings arise after working with smart assistants. Here it must be clarified whether a device was malfunctioning due to an application of smart assistants or due to the device itself. It makes a difference whether devices can be connected externally, for example with a kind of API or if direct access to the software of the devices is required. In such cases, it could be hard to prove when and why defects occur, because the software of the device has to be inspected. This could mean that the Source Code of the software must be disclosed, at least to courts or for expert evidence.

As other technical innovations and data-based business models, smart assistance in the Internet of Things will meet the challenge of the new General Data Protection Regulation that will become effective in May 2018 [Wy16] after a long negotiation process [Ho13a]. This new framework tries to establish common data protection requirements and enforcement mechanisms within the European Union. It aims, inter alia, at strengthening data subjects, introducing effective sanctions, proposing new mechanisms such as privacy by design [Ho13b] and data protection seals [HH15b], and at enhancing the cooperation of the data protection officers in the Member States [Al16]. However, the Data Protection Regulation still leaves many decisions up to the Member States, which makes it hard to realize this unity [Ro15]. Moreover, problems about smart assistants, big data, or cloud computing are not mentioned at all [RNR15]. Thus, there is a great need for research on the specific requirements for these and other innovative technologies, because companies need to be prepared once the new rules become applicable in 2018.

It is very likely that neither law nor technology alone are able to solve the privacy and data protection issues of smart assistants. There is a great need for an "alliance" of the two [Ro01]. Legal requirements serve as criteria for the design of specific technical and organizational solutions, so that the latter can comply with the data protection law from the very outset of the process of research and development (for examples, see [Ro11]). While working with smart assistants, it is almost impossible to avoid personal data. Therefore, a safe processing of these data has to be guaranteed in order to avoid restricting the users in their rights and, at the same time, losing their trust in innovative technical solutions.

5 The Entourage Research-Project

The challenges described above will be addressed over the next three years in the new research project "ENTOURAGE – Smart Assistance – Enabling Trusted Ubiquitous Assistance"[4] that has attracted funding from the German Federal Ministry for Economic Affairs and Energy (BMWi) through its "Smart Service World" technology competition.

The interdisciplinary project started earlier this year and is one of 16 successful projects selected from among 130 entries. Together, the industrial and research-partners[5] are developing and testing an open ecosystem to support smart, secure, and reliable assistance systems in the Internet of Things. ENTOURAGE provides a hub for data and services, functioning as the link between IoT-platforms and services. It unites technical, organizational, and legal components, which lays the groundwork for innovative open assistance systems.

In ENTOURAGE an open ecosystem is being developed that is interoperable on many levels. The ecosystem allows a legally compliant and optimized access to the future field of assistance systems through the establishment of technical standards and collaboration models for system and server providers.

The open platform developed within the project ensures the flexible connectivity between assistance systems. To give special consideration to the user acceptance of the developed solutions, the combination of relevant information of different sources is complemented by the consideration of data protection and security issues (also from the legal perspective). This aspect is central to the project.

By analyzing the market potential and deriving business models for suppliers and users, the economic viability of ENTOURAGE is pursued. Especially in an open ecosystem where different actors deliver and process data and offer services (in this case particular-

[4] www.entourage-project.de

[5] The ENTOURAGE team brings together experts from Robert Bosch GmbH, Fraunhofer IAO, CONWEAVER GmbH, HaCon Ingenieurgesellschaft mbH, the Technische Universität Darmstadt, the Universität of Kassel and is coordinated by the ENX Association. Other associate partners include BITKOM, TeleTrust, T-Systems, the city of Cologne and the transit network of Berlin-Brandenburg.

ly smart assistants) based on that data, the consideration of incentive and pricing models is necessary as this exchange can hardly be achieved otherwise. However, as of now such incentive and pricing models do not exist and should be developed on the basis of profound scientific analyses.

Moreover, ENTOURAGE develops a security assistant which supports users in the areas of login details, data access and data usage. This way, the security assistant contributes significantly to the user acceptance as it helps to handle challenges of data protection and usability. It also supports legal compliance when solutions based on ENTOURAGE are applied.

To verify and demonstrate the potential of ENTOURAGE, three pilot scenarios are planned. They are complementary and integrated into one ecosystem. First is the scenario "Automobile platforms and sustainable mobility". This scenario deals with the interaction of home, commercial, vehicle, and mobility platforms. It pursues the goal of an intelligent governance of the individual traffic at personal and system levels. The second scenario „Public transport and elastic infrastructures" includes among other aspects travel planning, which takes into account real time information, appointments, choice of modes of transport, and navigation information exchanged between platforms (smartphone, car, house), as well as additional services such as recommendations on the nearest gas stations or gastronomic possibilities. In the third scenario „Smart Home and Digital Life Balance" the question of how technical and planning components can help employees to keep a better life-work balance with the use of smart assistance is investigated.

6 Conclusion

In this position paper we have argued that while the Internet of Things enables innovative smart services and smart assistants that are much more powerful than before, there are still some challenges to be overcome to reach their full potential. As they are often neglected in the research and development of IT systems due to a focus on technical aspects, we have concentrated on non-technical challenges in this paper. Socioeconomic and legal aspects represent important framework conditions for the success of ecosystems for trustable smart assistants and therefore are discussed in greater detail. The main challenges for these ecosystems that have been identified and will be analyzed further in the ENTOURAGE-project and its pilot scenarios are summarized in table 1 (following page).

As this is a position paper, we were only able to present our understanding of the main terms and sketch out the basic challenges that we see from a socioeconomic and legal perspective for this relatively new area of research. As for a next step, a more thorough investigation of the issues presented will be performed in our new research project ENTOURAGE, which was presented in the last chapter. Feedback and discussion about the arguments presented in this paper will be highly valuable for our future research and the

success of the project.

Main socioeconomic challenges	Main legal challenges
• Functioning mechanism allowing for flexible integration of new actors • Economic viability of the ecosystem • Incentive and pricing models • Multi-sided market between different actors in the ecosystem • Strategies for market entry considering network effects • Interests of various stakeholders • Business models in the ecosystem	• Privacy risks of personal profiles and sensitive data in the Internet of Things • Addressing the problem of de-anonymization in big data • Strategies for data minimization • Applying the new General Data Protection Regulation to specific technologies and business models • Liability for unreliable data in software ecosystems

Table 1: Summary of the main challenges that have to be analysed

References

[Ac14] Acatech: Smart Service Welt: Umsetzungsempfehlungen für das Zukunftsprojekt Internet-basierte Dienste für die Wirtschaft. Berlin, 2014.

[Al16] Albrecht, J. P.: Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, Computer und Recht, pp. 88-98, 2016.

[CJ03] Caillaud, B.; Jullien, B.: Chicken & Egg: Competition among Intermediation Service Providers. The RAND Journal of Economics, 34(2), pp. 309-328, 2003.

[EHB11] Eppler, M. J.; Hoffmann, F.; Bresciani, S.: New Business Models Through Collaborative Idea Generation. International Journal of Innovation Management, 15(06), pp. 1323–1341, 2011.

[Ev03] Evans, D. S.: Some Empirical Aspects of Multi-sided Platform Industries. Review of Network Economics, 2(3), pp. 191–209, 2003.

[Gi07] Gitter, R.: Softwareagentensysteme im elektronischen Geschäftsverkehr: Rechtliche Rahmenbedingungen und Gestaltungsanforderungen an agentengestützte Assistenzsysteme, Baden-Baden: Nomos, 2007.

[GMW08] Glass, A.; McGuinness D. L.; Wolverton, M.: Toward establishing trust in adaptive agents. Proceedings of the 13th international conference on Intelligent user interfaces. ACM, 2008.

[GM02] Göker, A.; Myrhaug, H. I.: User context and personalisation. Workshop proceedings for the 6th European Conference on Case Based Reasoning, 2002.

[HG15] Hornung, G.; Goeble, T.: "Data Ownership" im vernetzten Automobil. Die rechtliche Analyse des wirtschaftlichen Werts von Automobildaten und ihr Beitrag zum besseren Verständnis der Informationsordnung, Computer und Recht, pp. 265-273, 2015.

[HH15a] Hofmann, K.; Hornung, G.: Rechtliche Herausforderungen des Internets der Dinge. In: Sprenger, F.; Engemann, C. (Hrsg.): Internet der Dinge. Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt, Bielefeld: transcript, pp. 181-203, 2015.

[HH15b] Hornung, G.; Hartl, K.: Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierung und -audit, Zeitschrift für Datenschutz, pp. 219-225, 2014.

[Ho13a] Hornung, G.: Die europäische Datenschutzreform – Stand, Kontroversen und weitere Entwicklung, in: Scholz, M.; Funk, A. (Hrsg.): DGRI-Jahrbuch 2012, Köln: Dr. Otto Schmidt, pp. 1-24, 2013.

[Ho13b] Hornung, G.: Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework, Innovation: The European Journal of Social Science Research, pp. 181-196, 2013, http://dx.doi.org/10.1080/13511610.2013.723381.

[Ka15] Kaufmann, T.: Geschäftsmodelle in Industrie 4.0 und dem Internet der Dinge. Springer, Wiesbaden, 2015.

[Li11] van Limburg, M.; van Gemert-Pijnen, J.; Nijland, N.; Ossebaard, H. C.; Hendrix, R.; Seydel, E. R.: Why business modeling is crucial in the development of eHealth technologies. Journal of Medical Internet Research, 13(4), e124, 2011.

[MR99] Mahler, A.; Rogers, E.: The diffusion of interactive communication innovations and the critical mass: The adoption of telecommunications services by German banks. Telecommunications Policy, 23(10/11), pp. 719–740, 1999.

[MV14] Moorthy, A. E.; Vu, K. L.: Voice activated personal assistant: Acceptability of use in the public space. Human Interface and the Management of Information. Information and Knowledge in Applications and Services. Springer International Publishing, pp. 324-334, 2014.

[Mu13] Muegge, S.: Platforms, Communities, and Business Ecosystems: Lessons Learned about Technology Entrepreneurship in an Interconnected. Technology Innovation Management Review, 3(2), pp. 5–15, 2013.

[OPT05] Osterwalder, A.; Pigneur, Y.; Tucci, C. L.: Clarifying business models: Origins, present, and future of the concept. Communications of the association for Information Systems, 16(1), pp. 1-25, 2005.

[Po99] Pouloudi, A.: Aspects of the stakeholder concept and their implications for information systems development. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences, pp. 1-17.

[Ro01] Roßnagel, A. (Hrsg.): Allianz von Medienrecht und Informationstechnik? Ordnung in digitalen Medien durch Gestaltung der Technik am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltschutz, Baden-Baden: Nomos, 2001.

[Ro11] Roßnagel, A.: Das Gebot der Datenvermeidung und -sparsamkeit als Ansatz wirksamen technikbasierten Persönlichkeitsschutzes? In: Eifert, M.; Hoffmann-Riem, W. (Hrsg.): Innovation, Recht und öffentliche Kommunikation, Berlin: Duncker&Humblot, pp. 41-66, 2011.

[Ro13] Roßnagel, A.: Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht. Zeitschrift für Datenschutz, pp. 562-567, 2013.

[Ro14] Roßnagel, H.; Zibuschka, J.; Hinz, O.; Muntermann, J.: Users' willingness to pay for web identity management systems. European Journal of Information Systems, 23(1), pp. 36–50, 2014.

[Ro15] Roßnagel, A.: Was bringt das neue europäische Datenschutzrecht für die Verbraucher – Die Datenschutzgrundverordnung steht vor ihrer Verabschiedung. Verbraucher und Recht, 10, pp. 361-362, 2015.

[RNR15] Roßnagel, A.; Nebel, M.; Richter P.: Was bleibt vom Europäischen Datenschutzrecht? - Überlegungen zum Ratsentwurf der DS-GVO. Zeitschrift für Datenschutz, pp. 455-460, 2015.

[Sc14] Scholz, P.: Kommentierung von § 3a, Rn. 17, in: Simitis, S. (Hrsg.): Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden: Nomos, 2014.

[SS14] Scholz, P.; Sokol, B.: Kommentierung von § 4, Rn. 3, in: Simitis, S. (Hrsg.): Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden: Nomos, 2014.

[SFG99] Sharp, H.; Finkelstein, A.; Galal, G.: Stakeholder identification in the requirements engineering process. In Proceedings of the Tenth International Workshop on Database and Expert Systems Applications, pp. 387–391, 1999.

[St05] Steidle, R.: Multimedia-Assistenten in Betrieb. Datenschutzrechtliche Anforderungen, rechtliche Regelungs- und technische Gestaltungsanforderungen für mobile Agentensysteme, Wiesbaden 2005.

[TF14] Thüsing, G.; Forst, G.: Beschäftigtendatenschutz und Compliance, 2. Aufl., § 17, Rn.15, 2014.

[Wy16] Wybitul, T.: Datenschutzgrundverordnung verabschiedet – die wichtigsten Folgen für die Praxis auf einen Blick. Zeitschrift für Datenschutz-Aktuell, EU, 8, 2016.

[ZA10] Zott, C.; Amit, R.: Business model design: an activity system perspective. Long range planning, 43(2), pp. 216–226, 2010.