THE INFLUENCE OF HANDLING META DATA ON PRIVACY AND THE ECONOMY

Elvira KUHN
University of Applied Sciences
Schneidershof, 54294 Trier, DE
kuhne@hochschule-trier.de

Udo BURCHARD
University of Applied Sciences
Schneidershof, 54294 Trier, DE

Abstract. *Nowadays, we produce a lot of Meta Data - hidden behind the primary proper data records - by using any kind of IT-equipment. We are using the primary proper data records exclusively, sometimes sending these to other people in a direct way or sharing the information on social media. Many people do not know about the existence of hidden personal information. But what is the reason for the existence of such information? The manufacturers themselves can make a lot of money in the tens of billions by collecting the data records, then consolidation and sell of the information. They themselves do not know exactly what the clients do with this data. The motivation of the buyers is to assess, monitor and influence the behavior of their clients or to send information about new products selectively to them. At last, the range of new products, as well as the innovation process, are influenced by this knowledge, too. But is all of this for the benefit of the private person? Or only of businesses? What is new? As a result of the handling process relating to Meta Data drafted above, we think that the discussion about the ownership of data records has to take into account the influence on privacy as well as on the economy. We show that this influence may shift if all actors know about the purposes of the hidden data and know what to do if they want to have leverage in this business. In this paper, we discuss these facts by using a study on private data sets as an outcome of using mobile phones, searching machines, and discount coupons. Based on this study we suggested a new definition of privacy under different aspects like privacy protection, intimacy, tracking life activities or well-being. At last, we offer a solution for the discussion on the ownership of data records, especially concerning the future of privacy and the loss of trust concerning the handling Meta Data by companies. For companies, we offer several possibilities to retain the trust of their clients.*

Keywords: *privacy; data mining; meta data; profile oriented marketing; ownership of data records.*

Introduction

In daily life, we use multiple kinds of IT-equipment, like a mobile telephone, Smart Phone, Laptop, tracking equipment, (for instance counting number of steps), facility equipment, like controllers for rolling shutter, door openers. The appeal to use these services is the comfort, similar to not having to go to the market but buying from your sofa whatever you want. Or even simply setting marks about what could be interesting. Even if you do not mark something, the time your cursor rests on an object reveals the

interest on the object. Sometime later you will find the object on another page of another website, for instance, presented on the page of your email-account. This is called profile oriented marketing. By seeing the object, we are remembered of our wish, and in many cases, the client will buy it. It seems so easy. And so comfortable. We accept this data transfer because we think we have nothing to hide.

On the other hand, we see that it is sometimes dangerous to give away private data sets. We know about bullying attacks on the internet against children. Sometimes it happens that we have just sent a picture from our holiday to friends, and then a short time later we find these pictures from our holidays posted on the social media platform sites of complete strangers without being asked for permission to publish. In this moment everybody can see and establish the connections between our friends, the places that we have visited, for example by scanning your face and then filter it out from all pictures existing on the internet, to figure out where you have been, at what time and with whom. After doing this, the person knows what you prefer, your special hobby, and they can sell this information to companies who use it to enable profile oriented marketing as has been shown (Reschreiter, 2017). Selling the collected information of different IT-platforms and other digital equipment connected via the internet about special groups of persons or about an individual person is the first step of the attack with marketing information or manipulation of the customer.

We show that a private person is not helplessly at the mercy of providers and players in internet technologies. On the other side, we also show that the careless handling of profile oriented marketing may be risky for businesses. At the end, we give a summary of measurements to avoid risks for both – for the individual as well as for the enterprise.

Methodology approach

Our aims are, on the one hand, to help a private person not to lose privacy by using IT based equipment, on the other hand, to open up undreamt-of possibilities for Business Management with these new technologies. To achieve our aims, the first step is to illuminate the technologies based on Web 4.0 as seen in several studies (Augusto & Huch, 2012; Dale, Higgins & Carolan-Rees, 2015; Mueller-Mielitz, 2016; Völkel & Lorbach, 2015). We show the State of the Art of the information market, which means answering these questions: What ways already exist to produce information, who is the seller and who is the client to buy this information? What is the motivation for both to deal with people's private information? As a result of this short market description, we have a base to discuss what is new.

Secondly, we discuss the trade of information and how much money an expert can make if there is no complete data set available. We show you that experts can draw conclusions on the basis of other data. For more details, see Frickel (2012) and Jewett (2017). Going on from this explanation report, we can discuss the dangers of losing privacy and the opportunities for Business Management to offer services for potential or existing clients.

In step three, we deal with the question of the influence of this knowledge on products and innovation processes. In this context, we give also answer to these questions: Is all of this for the benefit of the private person? Or only for businesses? At the end of step

three, we merge both aspects, losing privacy vs. losing trust in IT and draw conclusions for the handling of Meta Data. In addition, we discuss more risks concerning daily life.

At last, we explain the consequences and draw conclusions of what we can and have to do as a private person or as a manager. The results for an individual and for companies summarizes the cautious handling of Meta Data.

State of the art

We use IT based equipment in our daily life, and in doing so we produce Meta Data. Most users do not know about these data records and what is happening with these. Therefore, the users cannot decide who is allowed to use their data records and for what purpose. Some companies, such as METRO as Koch (2017) demonstrated, are newcomers on the information market. To avoid losing the trust placed in them by their clients, newcomers, as well as established companies like Amazon, Google, Facebook, need to recognize megatrends in the behavior of their clients.

Two ways to get information

From the point of view of companies, there is an easy way to get information: To collect it themselves by using so-called tags or to buy it from another company.

We explain now the collection of information by companies themselves, exemplified by a picture taken with a digital camera (Figure 1).

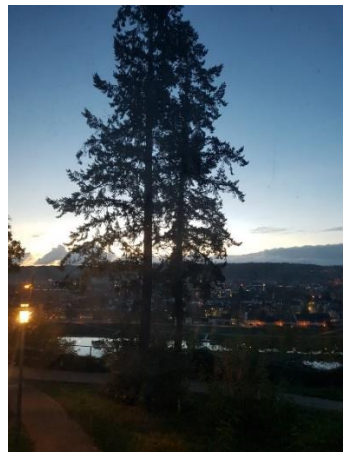

Figure 1. A Photo was taken with digital camera (author's own caption)

You can see a picture that we would like to send to our friends. But what kinds of information does it show? What will other people be able to infer about the owner of this picture, if somebody sent it to them? We upload the picture to http://regex.info/exif.cgi2. After a few seconds, this page shows us a map with our own position, and many other pieces of information, like the type of camera we use, GPS Latitude and Longitude, the date and time when we made this picture. In Fig. 2,

you can see this information called META DATA behind the picture – produced by the camera software itself.

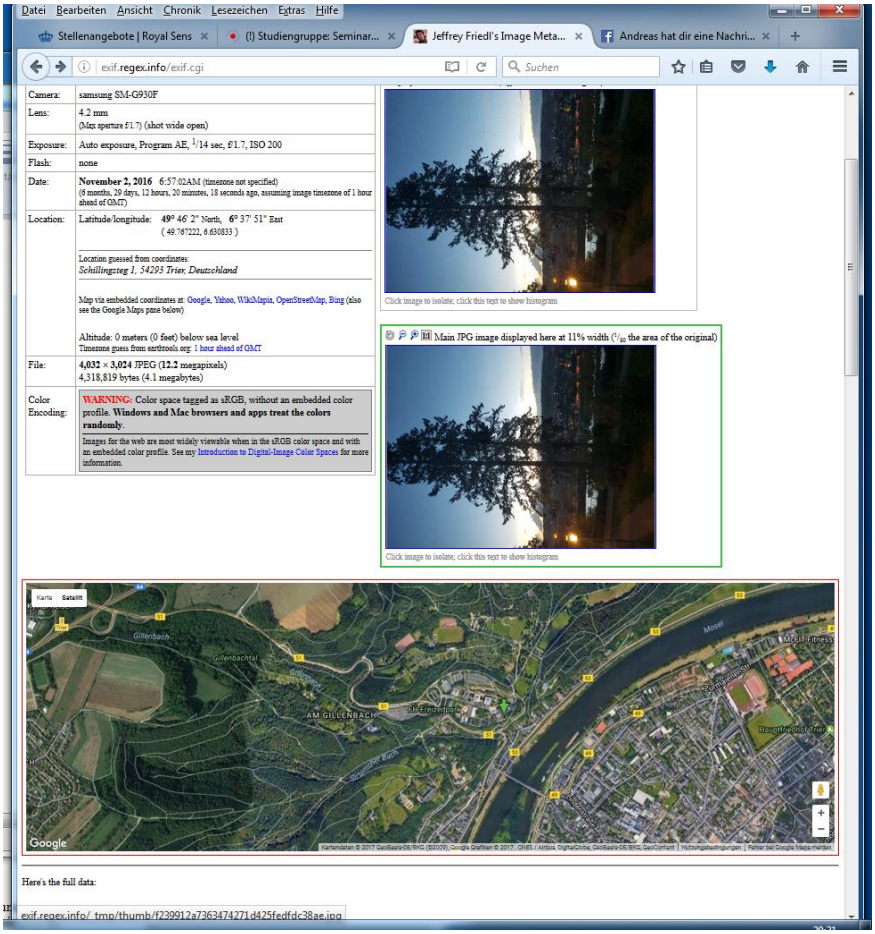

Figure 2. Hidden Information behind a digital photo by using tags (EXIF, 2016)

Many people have used this trick to commit crimes. The perpetrators have gathered information from the picture about the exact position of the vehicles, which are for sale on special online pages. Then, the vehicles were stolen at certain times when the owners did not indicate any accessibility, arguably, because they are currently not at home. As you can see, if the data set will fall into the wrong hands, it will be dangerous for you or your possessions.

There are many ways to access Meta Data. This is a type of data, which was never intended for the use of human agents, but for the purpose of digitally automated indexation, processing or cataloguing the message/picture/clip/audio file etc. In many cases, this concerns so-called header data. For music, images, and videos, EXIF headers are often attached to the actual file. The build of the header is structured in tags and contains information about the recording source, the recording location, the recording time and the creator. The data is saved automatically and unsolicited by the recording device (e.g. smartphone camera), without the knowledge, approval or admission of the

user. The visualization of this information with special tools is fairly easy even for laymen and might be used in committing cybercrimes.

The second way to gather information concerning the behavior of clients is to buy it. With the daily use of search engines and IT equipment, data of the users is logged and summarized to a data set. These data sets do not only generate a financial added value for marketing purposes in-house but can also be sold to target groups linked with external companies. Information leadership is an enormous competitive advantage. Based on this knowledge, we have created a database with different tables to collect data, such as GPS-Data integrated into each Smartphone or mobile telephone, in combination with a time stamp, SSID Dataset, name, EC-card, address – which you have to give to retailers when buying with an EC-card.

Figure 3. Platform with the table of data (Sterk & Eichhorn, 2016, p.5)

Figure 3 shows one of the tables created within our studies. These tables contain data sets which you will produce alongside when using your mobile telephone, google as a search engine for the internet or trading stamps. In our study with the objective to learn more about the private life on weekends, we wanted to know which Apps the students use, which google seeking words they insert or which numbers they call with their mobile telephones or Smartphones and how they would usually transmit information. For example, when using mobile telephones, they can send SMS or connect to WLANs. We thought that if all of this information will be protocolled, we could make conclusions about their behavior. By using Apps like Facebook or WhatsApp, everybody can find out who our friends are and they can develop a notion about our social life. Often many people publish their social and political opinions on forums or social media sites like Facebook. When doing this, the whole world can see and retrieve it. We wanted to collect data from browser sessions to see their interests, too. As an example, the use of Apps, like Deutsche Bahn or means of public traffic reveal where we want to travel. Logging all of these actions in combination with a time stamp and IP address, we can infer the daily life rhythm of a person. Unfortunately, it

was too much work to collect the data by hand, so we have not had a lot of data but only some. Here, we only want to show what you can do with the daily produced data from your usage of IT.

The collected information on interests e.g. in books, shows or events allows for more than just generating APPS-attacks. A company's marketing department is able to pool this information with intel facilitated by the provider (such as GOOGLE) and the client´s profile. From the point of view of the company the client is lucent

The new information market

With the access to certain websites, and especially in the area of e-commerce, user behavior and user data are continuously saved. On the one hand, personal data like names, addresses, account information, and on the other hand accompanying data like geo-coordinates, interests and purchase behavior are recorded and evaluated. When using discounts or participating in collection campaigns, also numerous data is collected. The participants already consented to the transmission of their data in the participation form. Also, common knowledge in this regard is the selling of user data with the highest possible profit to third parties, whereby the customer only gets a small benefit. Most of the normal users only access the primary proper data records, they do not know about the existence of hidden personal information. The market for this is estimated to be in the tens of billions. The sellers only collect the data records and sell them without asking about the intended usage. Nobody outside of the companies buying the data sets knows what will happen with the data, how it is stored and archived, and who has knowledge of it. The company ElevenPath offers a tool called FOCA (Fingerprinting Organizations with Collected Archives) to collect META DATA from documents in DOCX and PDF format, as described by Kuksov (2017). The usage of this tool can be seen by the owners of homepages as cybercrime.

The new relationships between different data sets

In order to decide whether the creation of new data relations between different data bases and the new conclusions based on them is dangerous or not, we explain the main methods and techniques in data sciences.

The term BIG Data designates the collection of data from various areas, like e.g. the Internet, mobile communication, social media, credit cards, customer cards and smart meeting systems and vehicles, as well as their processing and evaluation (see, for instance, Crisan, Zbuchea & Moraru, 2014). The data volume increases climactically faster, because not only manual data is included, but in the frame of digitalization also automatically generated Meta Data is saved.

Consolidation Data Set is a data set which contains not necessarily only original data but also data estimated or deduced from BIG Data sets. The idea is to use consolidation, evaluation, and correlation in order to transform the data into an appropriate format regarding the context. These data packages are called data sets. The clustering of data can be an appropriate form of consolidation. Here, data sets are summarized and evaluated again according to defined characteristics.

The gathering techniques in networks result in completely new types of structures, interfaces, and links between world wide data bases and services. With the help of Data Mining, you can descry new relationships between known data sets. To spot new relations between different data sets opens a vast great treasure chest of knowledge about the individual. Data Mining is a set of statistic methods on big data sets with the target to create new relations and trends. The IT provides the appropriate resources in the form of numerous tools for this purpose. The goal is to process the data from the most various sources with the most various formats. For this purpose, corrupt or incorrect data is recorded as fast as verified data by the algorithms. Due to the consolidation process, errors can be located and rectified, missing data can be interpolated or logically incorrect data can be removed.

Digression: How reliable are the processes?

If they are reliable, what happens with incorrect or corrupt data? Based on inaccurate data sets, we are employing exact analyses processes, but the result is still incorrect. For security-relevant data - as in medicine - or under the aspect of high availability (by Six Sigma, as has been shown Rowlands, Price, George and Maxey (2016), a smaller, but more reliable data base should be used. For less vulnerable analysis, the easier and not verified evaluation is conceivable, for example with e-mail advertising campaigns.

New conclusions can be compared to Chinese whispers. What is the result at the end? The currently possible conclusions are not more reliable than before. A bigger amount of data, especially in the most various formats, is not necessarily the basis of more reliable data. As seen in Kessel and Vogt (2016, p.157) especially for BIG DATA, “the effort to verify the data is very high”.

The frequent occurrence of incorrect information can lead to a false sense of reliability, a common danger. A current example would be the fake news that can be found circulating in social networks. With the help of specific information, a profiling will be undertaken, that serves the purpose of manipulating coherent target groups with precision, e.g. by advertisements. By the acquisition of person-related data, weak points are utilized by criminal groups.

A few years ago, collecting exact keywords, keys and also indexing people, were activities that had to be carried out during searches on the Internet and when storing data in databases. Today similar and identical products and contents of the same group are represented by intelligent algorithms, but also complementary and combinable results are displayed, which are similar and easily supplemented.

Discussion

As you can read in (Sterk & Eichhorn, 2016), in the first part of our study we have discussed the consequences of one person knowing all of this information and how they can employ it. All students had thought that everybody might as well have all of their information because they have nothing to hide. But in a discussion only a week later, concerning the wanted information from all students some declined because they did not have any trust in the person who would be able to discern individuals reversely from the data set. Later, as we solved this problem by using a secret web side, they

were disgruntled about the lecturer knowing too much about their private lives. The provider who is collecting the data in real life is perhaps unknown, but the people who are buying this data from providers like Amazon, Google, Facebook to analyses it with business intelligence techniques, could be someone you know of your time at the University. The next problem was the storage of the data set and the guarantee of administrated data access. This is a very new problem with the internet, mobile phone or selling marks.

The new information market

What is new in this market? We do not know which data will be saved and generated while using the software at any point. We do not know where the data is saved. We do not know who the owner is. We do not know what happens with it. We do not know; in the case, we wish to delete the data that this will be done or whether it is even possible to execute. We do not know whether the data set is adequately secured and access is only possible with authentication.

The market is very non-transparent. The new information market is not made for the common citizen. Therefore, we demand more transparency. For these reasons, we no longer employ the phrase *anonymization of data*, but pseudonymisation, according to Ganslandt (2017).

It seems that the market will be manipulable. Recently, we learned that GOOGLE has manipulated the offered shops on their web pages, rigging them in their favor as Kottasová (2017) demonstrated. An old saying goes: Money corrupts. Companies with money monitor the innovation process and shape with this the future, too. So, the whole economy will be influenced. If the great players on the information market have a wish they are able to push it. Still, they have the power to put pressure on all citizens. Because of so much unknown handling, we cannot say what is true and what is not. But who is the falsifier? As we have shown, the answer lies in the methods and handling of data. Handling means that the data set is generated covertly and without any guarantee of effectual precautions against data abuse.

Conclusions

Now it´s time to think about what we all can do against this horrible reality. Looking at the questions written in the discussion section, we deduce consequences from these.

One consequence for data security officers within companies is the necessity of using all available resources to secure all handling by using specialized software. For example, certain functions within Microsoft Office, like Document inspector (Microsoft Virtual Academy, 2017) can help with that objective. With the help of this function, the user can see all data included in the file. The data set can now be deleted on demand, but not the embedded data. In the rules of action, the data security officer should be state and communicate that you have to be careful when inserting pictures and diagrams. As seen in Kuksov (2017), with the help of DLP (Data Loss Prevention) module in Kaspersky Total Security for Business, Kaspersky Security for Mail Server and Kaspersky Security for Collaboration Platforms, one can delete confidential Meta Data like change protocol, comments, and embedded objects.

In our handling of IT or with our private data set, we follow the rules of action. There is a need for a platform to help in the case of and warn about cyberattacks (for example with generated emails) and inform people about what steps to take when it happens. Better yet would be to install preventive measures and to prohibit the producing or collecting of data, for example with cookies. Also, it is helpful to tout as written in Danezis, Domingo-Ferrer & Hansen (2015) as well as in Dratwa (2014).

Possible consequences for the political handling could be the augmentation of fines and combining them with a personal imprisonment for data providers if they do not disclose openly what they collect. It should be legally clarified that the producer is the sole sovereign decision maker on distribution. If they cede the right to preside over data, then immediately there has to be a check on whether the data may be used as an aggressive tool against the freedom of anybody. In this case, if there is any possibility to fill out the lack within a data set as explained before, it is not allowed to use this data anymore. To observe the right handling of data sets there is the necessity to install some observers to control whether the memory places are pursuable and known. If there is any upload of data the owner has to know it (if not, it is a theft), but as said before not only they. Before any transfer can happen, the provider has to declare to whom he will give the data, and the seller has to report what he will do with it, and later on what he has done, where the archive is and at what time he will delete it. It must be forbidden to trade with third parties, and only consolidated data can be tradeable. In Heidrich and Hansen-Oest (2016) we have found the statements about the rights of deleting data directly by the record place. Actually, the European court has only postulated the right of the block from personal results of seeking machines. If a company has data from a person published by itself, it has the obligation to inform all stations about the claim of cancellation of the person concerned. In Article 22 EU Law (2016) is written: „Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect."

In new information market, democracy is receding. The reason for that is that the distribution of information is carried out in a profile oriented manner. Today, the price of shoes, flies and everything else is dependent on your profile, depending on the profile you might get information or not. This means to paternalism and patronizes citizens. The trust in IT is diminished. "We need data sovereignty" as seen in Dräger (2017, p.84.) For business managers, it is important to "see the mega trends" (Gernandt, 2017, p.68). He is discussing the addictiveness of the business strategy on new behaviors and expectations of clients in this article, and says "because to do the right things decide the market". "According to Darwin's On the Origin of Species as found in (van Wyhe, 2002), it is not the most intellectual of the species that survives; it is not the strongest that survives; but the species that survives is the one that is able best to adapt and adjust to the changing environment in which it finds itself." We recommend business managers to use an open communication standard on profile oriented marketing.

Summary and outlook

Trepte and Masur (2017) sustain that privacy is a very important value for the individual as well as for the society We have reached the end of privacy, because of our fundamental law in according to Kant „My freedom ends, where I touch upon the freedom of another" (in Vieweg, 2016). Therefore, I cannot trade with any Meta Data generated through my actions, since the consequences on whose rights may be violated are unforeseeable.

Take away their power. The same way you would react to a real world situation, in which someone tries to sell you a product you do not want or need, with classical advertising, letters, annoying phone calls and others, by ignoring them completely, is how we as consumers can get rid of this problem once and for all. By using a spam filter, never participating in any discount campaigns or filling out loyalty cards we can take back our own informational sovereignty. Nothing is free in this world, the massive profits of the information industry pale our meagre deductions. Elucidation on the consequences of our daily actions changes people's behavior in handling their data, according to our study. It is essential for business managers to keep empowerment, adaptiveness, and megatrends in mind. An open communication about the information market or the selection of another form of acquiring new clients are possibilities of securing the future of the company.

Acknowledgements. *We give many thanks to* ***t****he students, visiting the seminar of Prof. Kuhn, University of Applied Sciences, in 2016, because this paper is based on unpublished presentations by students and the results of their studies.*

References

Augusto, J.C., & Huch, M. (2012). *Handbook of Ambient Assisted Living, Technology for Healthcare, Rehabilitation and Well-being*. Amsterdam, Berlin, Tokyo, Washington, DC: IOS Press.

Crişan, C., Zbuchea, A., & Moraru, S. (2014). Big Data: The Beauty or the Beast. In C. Bratianu, et al. (Eds.), *Strategica: Management, Finance, and Ethics* (pp.823-840), Bucharest: Tritonic.

Dale, M., Higgins, A., & Carolan-Rees, G. (2015). Sherlock 3CG® Tip Confirmation System for Placement of Peripherally Inserted Central Catheters: A NICE Medical Technology Guidance. *Applied Health Economics and Health Policy*, 14(1), 41-49.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Metayer, L., Tirtea, R., & Schiffner, S. (2015). *Privacy and Data Protection by Design*. Retrieved from https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.pdf/

Dräger, J. (2017) p.84., Individuelles Lernen durch Digitalisierung. in Palais Biron, Baden Badener Unternehmer Gespräche, Nr. 25, Sommer 2017.

Dratwa, J. (2014). *Ethics of security and surveillance technologies, European group on ethics in science and new technologies to the European Commission*. Retrieved from http://www.forum-privatheit.de/forum-privatheit-

wAssets/docs/literaturhinweise/2014EuropeanGrouponEthicsinScienceandN.pdf.

EU Law (2016). On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Regulation (EU) 2016/679 of the European Parliament and of the Council. Retrieved from http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.DEU&toc=OJ%3AL%3A2016%3A119%3ATOC.

Frickel, C. (2012). *Der Datenkrake: Was Google schon jetzt alles über Sie weiß, Fokus online.* Retrieved from http://www.focus.de/digital/internet/google/tid-27798/datenkrake-was-google-ueber-sie-weiss-was-weiss-google-alles-ueber-sie_aid_843777.html.

Ganslandt, T. (2017). *Aufbau von Datenintegrationszentren*. Paper presented at CONHIT 2017, MIRACUM-Konsortium, Berlin.

Gernandt, K. (2017). Das Ende der Strategie. Palais Biron, Baden Badener Unternehmer Gespräche, 25, Sommer 2017, 68.

Heidrich, J., & Hansen-Oest, S. (2016). *Welche Änderungen die neue EU-Datenschutz-Regulierung in Deutschland bringen wird.* Retrieved from https://www.heise.de/ct/ausgabe/2016-9-Welche-Aenderungen-die-neue-EU-Datenschutz-Regulierung-in-Deutschland-bringen-wird-3166896.html 166.

Jewett, E. (2017). *Voraussetzung für erfolgreiche Big-Data-Analyse: Korrekte Daten und Transparenz*. Retrieved from http://www.searchenterprisesoftware.de/sonderbeitrag/Voraussetzung-fuer-erfolgreiche-Big-Data-Analyse-Korrekte-Daten-und-Transparenz.

Kessel, T., & Vogt, M. (2016). *Fit für die Prüfung*: Wirtschaftsinformatik, Lernbuch, UVK Verlagsgesellschaft mbH, Konstanz und München. 157.

Koch O. (2017). Wege in die digitale Welt. Palais Biron, Baden Badener Unternehmer Gespräche, Nr. 25, Sommer 2017, 72.

Kottasová, I. (2017). EU slaps Google with record $2.7 billion fine. Retrieved from http://money.cnn.com/2017/06/27/technology/business/google-eu-antitrust-fine/index.html.

Kuksov, I. (2017). Wie flüchtige Metadaten für echte Probleme sorgen können. Retrieved from https://blog.kaspersky.de/office-documents-metadata/9915/

Microsoft Virtual Academy (2017). *Document inspector.* Retrieved from https://msdn.microsoft.com/en-us/vba/office-shared-vba/articles/using-the-document-inspector.

Mueller-Mielitz, S. (2016). *Assistenz*-Erleben – das Spiel-Konzeption einer nutzerzentrierten Alltagsunterstützenden Assistenz-Lösung (AAL), IEKF GmbH.

Reschreiter, R. (2017). *New Insights of Profile Oriented Marketing and Adaption Management for a Future-Oriented City Development.* Retrieved from http://researchleap.com/new-insights-profile-oriented-marketing-adaption-management-future-oriented-city-development/.

Rowlands, D., Price, M., George, M.L., & Maxey, J. (2016). *Das Lean Six Sigma Toolbook, Werkzeuge zur verbesserung der Prozessgeschwindigkeit und–qualität.* Münich: Verlag Franz Vahlen GmbH.

Trepte, S., & Masur, P. (2017). Privacy attitudes, perceptions, and behaviors of the German population: Research Report. In Friedewald et al. (Eds.), *Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. [Forum Privatnes and self- determined live in the digital world].* Retrieved from https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-des-forums/Trepte_Masur_2017_Research_Report_Hohenheim.pdf.

Perghel, R., & Psychogios, A.G. (2013). Making sense of crisis: cognitive barriers of learning in critical situations. *Management Dynamics in the Knowledge Economy*, 1(2), 179-205.

Pew Research Center (2012). *Social networking popular across globe.* Retrieved from http://www.pewglobal.org/files/2012/12/Pew-Global-Attitudes-Project-Technology-Report- FINAL-December-12-2012.pdf.

Sterk, I., & Eichhorn, D. (2016). Gefahren durch Datenmissbrauch, Thema: Datengewinnung durch Analyse von Internetnutzung und Mobilfunk [*Studies about the handling of private data records*.] Intern paper, University of applied science, Trier, Department of Economy, Seminar Organisation und Informationsmanagement.

van Wyhe, J. (2002). *The Complete Work of Charles Darwin Online*. Retrieved from http://darwin-online.org.uk/

Vieweg, K. (2016). *Die Philosophie in Star Trek.* Ludwigsburg: Amigo Grafik.

Völkel, F., & Lorbach, I. (2015). *Smart Home - Bausteine für Ihr intelligentes Zuhause.* Freiburg: Haufe Verlag.