Data Privacy

This paper will describe what the current state of privacy is like in the world and how it can affect people and their safety and privacy as well as how one should be encouraged to help fix the issues with Big Data. Theoretical perspectives are examined, and these empirical findings will be described regarding data and information privacy and how it can be grouped according to privacy’s role in society, and the economics of privacy. The correct precautions and protection of data privacy creates a difficult situation to where it requires a careful analysis of what would really need to be kept private and what to be public. Over the years there has been multiple definitions surrounding data privacy from traditional *syntactic* privacy definitions.

“*Which capture the protection degree enjoyed by data respondents with a numerical value, to more recent semantic privacy definitions, which take into consideration the mechanism chosen for releasing the data*.”( Samarati,2012,pg,793).

The public needs to be aware to be able to learn the types of information that can be taken from all sites which are used and other electronic means and how the data is retained, how it is used, and what is shared with third parties. The same information must be available from those third parties. (Hanna,2018,pg,58).

“*All data collection mechanisms must be disclosed to users, including web beacons or other mechanisms for tracking user activity or data. This information must be sufficient for users to be able to identify and pursue disclosure and controls related to these data collectors.”* (Hanna,2018,pg,58).

Each website and application must disclose any ongoing content placed on the user’s device, as well as the uses of that content.(Hanna,2018,pg,58).

”*The potential risk to privacy is one of the greatest downsides of big data. It should be taken into account that big data are all about gathering as many data as possible to extract knowledge from them.”(* Ferrer, J,2015,pg,22).

In current years the idea of big data has become topical. There has been an increase in the amount of big data and so increases the chance of breaching the privacy of individuals. Since big data require high computational power and large storage, distributed systems are used. (Mehmood et al,2016,pg,1821). There are many parties that are involved in these systems and so the risk of privacy violation is increased. “*There have been a number of privacy-preserving mechanisms developed for privacy protection at different stages (e.g., data generation, data storage, and data processing) of a big data life cycle*.” (Mehmood et al,2016,pg,1821).

When looking at big data and privacy it is good to look at how Western scholars, and a handful of Chinese scholars have argued the protection of data is a necessity in order to have more freedom and escape the capabilities of big data. However, most scholars have made a point in how :”*this also obviously reflects the whole cultural background in China and predominant values that take society and the collective good as the first moral standard*.” (Yao-Huai, L,2005,1pg,13).

In fact, even with regards to this, it has been seen that, Chinese researchers also take different approaches than their Western counterparts. (Yao-Huai, L,2005,1pg,13). Chinese researchers will tend to argue on how the social function of privacy protection in relation to social order. Moreover, western scholars, such as Gavison, are encouraged to focus on the point that privacy is a need for democratic government.(Yao-Huai, L,2005,1pg,13).

*“Privacy Information privacy is the privilege to have some control over how the personal information is collected and used. Information privacy is the capacity of an individual or group to stop information about themselves from becoming known to people other than those they give the information to.*”(Gyanchandani,2016).

One could note that it is a serious user privacy issue. (Gyanchandani,2016). Data privacy is looked at through the use and governance of individual data and then setting up things such as policies in place to ensure that people’s personal information is collected in only appropriate ways. (Gyanchandani,2016).

“*Security concentrates more on protecting data from malicious attacks and the misuse of stolen data for profit. While security is fundamental for protecting data, it’s not sufficient for addressing privacy*.” (Gyanchandani,2016).

One can put data and security into two different ideas. First of all, there is problems that organically originate : Someone could upload a media that could incriminate themselves or others and create a dangerous situation that causes damages. (Von Voigt,2012,pg,1). A typical example of this category is someone uploading bad pictures of themselves into a public album instead of a private one or onto their timeline instead of a possible private message. There is a high possibility of damage being done to themselves or others . Usually when these cases happen it is very obvious since the link between the content and the user is direct, and the audience has direct interest in the content. (Von Voigt,2012,pg,1). One particular problem is that not everyone knows what is considered damaging content and from user to user that can and often does change over time. This is a serious problem, especially amongst the current generations. (Von Voigt,2012,pg,1).

Secondly, we have the Big Data problems created by others: there has been an emerging threat to users' online privacy which comes from others using media and using it to attack others or steal their media for their own use. This causes problems because of the fact that the person harmed is not involved when things are uploaded and then it becomes only a problem when it’s too late for them as the person in trouble has no idea of what’s been going on. (Von Voigt,2012,pg,2). As well as thus, there are currently no countermeasures, except in the case of post-priority legal matters, to prohibit others from posting potentially damaging information about someone. There are two conditions that must be met for this type of privacy threat to be effective: To begin, a piece of media must be able to be associated/linked to a person in some way in order to cause harm to that person. This connection might be non-technical, like being recognized in a photo, or technical, like a profile being linked to a photo. (Von Voigt, 2012, page 2) This metadata does not directly produce a technical link to a profile, but it does allow search engines to index and search the material, resulting in a technical link. Secondly, the content in question must include detrimental consequences for the individual who is connected to it. This can be non-technical as well, such as being portrayed in a compromising light. It can also be technical, which is more interesting. Metadata or linked data causes harm in several situations. Time and location data, for example, can reveal whether a person was in an embarrassing location, attended a political event, or was not where they claimed to be. (Von Voigt,2012,pg,3). Since the uploading of this type of damaging media cannot be effectively prevented, awareness is the key issue in combating this emerging privacy problem. (Von Voigt,2012,pg,3).

The field of data has an importance to be examined. This is because on the normative level in light of the information and society, one might expect data privacy as a component of data collecting. (Andrew,2014,pg,197). This is done through certain types of algorithms. These privacy-preserving algorithms use noise addition to alter original transaction of data. (Gyanchandani,2016) .

“*Therefore, the possibility that an untrusted cloud service provider infers the real frequent item set remains in the method . Despite the risk of association rule leakage, provide enough privacy protection because this privacy-preserving algorithm is based on “hiding a needle in a haystack””* (Gyanchandani,2016).

According to Henry (2009,pg,300), there could be a possible method through using some sort of vanish system in things like emails. This has been made through apps like snap chat. This could be useful to take same ideas and replicate it into other apps. (Henry et al,2009,pg,300). A possible way to implement these would be: An approach that one would require the allowing of one or more trusted third parties which display which information is necessary to gain access to databases and information. The third parties would be able to destroy the excess data after a period of time.(Henry et al,2009,pg,300).

If a user does not want uncontrolled media of themselves to be online, these various sorts of watchdog services can help to decrease the quantity of relevant pieces of media that they must keep an eye on. The details are disclosed, however, because this type of service can have major privacy concerns if created incorrectly. (Von Voigt, 2012, pg.1). Varied users have different usage and privacy requirements; thus, care must be taken to accommodate them. The fact that a user must give location information to the watchdog service in order to request relevant media is a key concern. (Von Voigt, 2012, pg.1).

Because the correlation between the location query and the user account is direct, there is little that can be done to protect the user's location privacy when using this type of service. An obfuscation strategy is one way to safeguard privacy to some extent. (Von Voigt, 2012, pg.2). A number of bogus inquiries could be issued for every actual inquiry, making it more difficult (but not impossible) for the SN(social networks) provider to determine the true location. This strategy, however, does not scale well for two reasons. For starters, it puts more strain on the SN. If enough requests are sent, however, the possibility of determining the genuine location increases, unless considerable care is taken in generating the bogus pathways and disguising the source IP addresses. (Von Voigt, 2012, pg.2).

GDPR is beneficial for data protection, however this isn't the case everywhere. The GDPR creates a statutorily protected data user privacy bill of rights throughout the Eurozone because it applies to all enterprises, regardless of location, who offer goods or services in the EU or monitor the activities of EU data users. (Koenig,2017,2018,pg.376). Corporations outside of Europe have no viable alternative that is like the GDPR system . (Koenig,2017,2018,pg.376). The Directive's fundamental principles and standardized EU data protection regulations provided a relatively straightforward blueprint for new EU member states and then the rest of the globe (Peyser,2019,pg,812). There may be a need for this to be put in other continents such as the USA.

W3C is another way of insuring data is correctly monitored and protected when it comes to computers. The World Wide Web Consortium's (W3C) proposal for an international standard for online privacy, as well as the effort to offer technology to support Web privacy, includes the Platform for Privacy Preferences Project (P3P) (P3P, 2000). The P3 Project intends to create a set of tools and services that give users more control over their personal data while also improving trust between Web services and individuals. P3P allows Web sites to express their privacy policies in a standardized format that the client computer can parse. (Steinke, pg. 198, 2002).

With data privacy, standardization of data transfer and storage will lower the IoT market's entry barriers. For example, several important industries have joined the All Seen Alliance (https://allseenalliance.org) standards effort in the IoT area. (Zumaya, pg. 37, 2015). It's critical to create a regulatory body for the Internet of Things, comparable to the World Wide Web Consortium, to oversee standardization and certification processes. Communication, device descriptions and discovery, data interchange, encryption, user consent procedures, and data modelling, storage, and routing are all essential areas for standardization. As previously indicated, standardization initiatives must be accompanied with a certification procedure. Individual companies are currently seeking to certify devices and apps on their own. (Zumaya, pg. 37, 2015). Sadly, such measures will obstruct interoperability. The IoT's certification method would be comparable to that of the Internet's certificate authority paradigm. The IoT certification paradigm, would be a possible way to attempt to improve data privacy and protection in standardization of data collection.

The IoT certification paradigm, on the other hand, would be significantly larger, as it could need to verify both hardware and software services. (Zumaya, page. 37g., 2015)).User privacy must be secured and enforced from the time data is recorded by sensors integrated in IoT solutions to the point where knowledge is extracted, and raw data is permanently and securely erased. (Pg. 38, Zumaya, 2015). The technology’s limitations will require stringent laws and regulations, as well as severe punishments for violators and misusers. (Pg. 38, Zumaya, 2015).

To sum up, future study issues that exemplify a multidimensional approach, blending the numerous interconnected concerns that appear in contemporary privacy questions in data, can be highlighted. (K et al, pg.155, 2016). Additional work in this area is vital and needed since data privacy issues influence internal and external stakeholders in a variety of ways, some of which may be unexpected.

“*These methods can extend our knowledge and provide new tools for enhancing health and wellbeing. However, they raise questions about how to best address potential threats to privacy while reaping benefits for individuals and to society as a whole.”(* Mulligan et al, 2015,pg,253).

The increasing trend of geo-tagged social media has big data privacy problems. (Von Voigt, 2012, pg. 6). Ideas were provided for how this location data can actually help users stay in control of the flow of potentially damage from misuse of social media. GDPR will enable the availability of data for safer use and , moreover may cause problems in terms of attempting to collect their own data from another entity. People also have the right to data privacy and have the right to be forgotten. Examples would be people who are targeted in the media about events relating to their life or connections to people they do not want to be associated with. They would no longer be a data subject and have all personal data deleted from the internet.

Bibliography

Martin, K., & Murphy, P. (2016). The role of data privacy in marketing. Journal Of the Academy of Marketing Science, 45(2), 135-155. Doi: 10.1007/s11747-016-0495-4

Abid mehmood1 , Iynkaran natgunanathan1 , Yong Xiang1 , (senior member, ieee), Guang Hua2 , (member, ieee), and song guo3 , (senior member, IEEE), Special section on theoretical foundations for big data applications: Challenges and opportunities, Protection of Big Data Privacy ,1821-1834, 1School of Information Technology, Deakin University, Victoria 3125, Australia 2School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 3Department of Computer Science and Engineering, The University of Aizu, Fukushima 965-8580, Japan Corresponding author: Y. Xiang (yxiang@deakin.edu.au, received February 29, 2016, accepted April 9, 2016, date of publication April 27, 2016, date of current version May 9, 2016. Digital Object Identifier 10.1109/ACCESS.2016.2558446

Data privacy law: an international perspective By Lee Andrew Bygrave Oxford: OUP, 2014, 272 pp, £75.00, ISBN 978-0199675555 (hbk),196-199

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: a technological perspective and review. Journal Of Big Data, 3(1). Doi: 10.1186/s40537-016-0059-y

Yao-Huai, L. (2005). Privacy and Data Privacy Issues in Contemporary China. Ethics And Information Technology, 7(1), 7-15. Doi: 10.1007/s10676-005-0456-y

Horvitz, E., & Mulligan, D. (2015). Data, privacy, and the greater good. *Science*, *349*(6245), 253-255. Doi: 10.1126/science.aac4520

Roxana Geambasu Tadayoshi Kohno Amit A. Levy Henry M. Levy, vanish: Increasing Data Privacy with Self-Destructing Data , University of Washington {Roxana, Yoshi, levya, [levy}@cs.washington.edu,299-350](mailto:levy%7d@cs.washington.edu,299-350)

De Capitani di Vimercati, s., Foresti, s., Livraga, g., & Samarati, p. (2012). Data privacy: definitions and techniques. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *20*(06), 793-817. Doi: 10.1142/s0218488512400247

Jim Isaak, IEEE Computer Society Mina J. Hanna, Synopsys,2018, User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection,56-59

M. Smith, C. Szongott, B. Henne and G. von Voigt, "Big data privacy issues in public social media," 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), 2012, pp. 1-6, Doi: 10.1109/DEST.2012.6227909.

Soria-Comas, J., & Domingo-Ferrer, J. (2015). Big Data Privacy: Challenges to Privacy Principles and Models. *Data Science and Engineering*, *1*(1), 21-28. Doi: 10.1007/s41019-015-0001-x

Michael l. Rustad\* & Thomas h. Koenig, 2017,2018, towards a global data privacy standard, 365-453

Paul M. Schwartz, Jefferson E. Peyser , global data privacy: the EU way, 2019, Professor of Law, UC Berkeley School of Law; Director, Berkeley Center for Law & Technology, 771-818

Gerhard Steinke, Data privacy approaches from US and EU perspectives, Telematics and Informatics, Volume 19, Issue 2,2002, 193-200, ISSN 0736-5853

C. Perera, R. Ranjan, L. Wang, S. U. Khan, and A. Y. Zumaya, "Big Data Privacy in the Internet of Things Era," in IT Professional, vol. 17, no. 3, pp. 32-39, May-June 2015, Doi: 10.1109/MITP.2015.34.