Privacy in the toolbox of freedom

Mandy Balthasar
Bundeswehr University Munich
Computer Science Department
Neubiberg, Germany
Mandy.Balthasar@unibw.de

Armin Gerl
University of Passau
Chair of Distributed Information Systems
Passau, Germany
Armin.Gerl@uni-passau.de

***Abstract*— A life can be mastered by digital processes in a world that is always incomplete due to its complexity, only by balancing. An ethical balancing act within the framework of Poppers' trilemma of open society. This is accompanied by another tightrope act between privacy, which is made visible, and privacy, which is technically implemented. In a social, digitally transformed data culture, privacy is always subjective from the user's point of view, which is why the degree of protection must be individually adaptable. As a key element between users, companies (technologies) and the legal frameworks, privacy languages should serve to give the user the freedom to control and manage transparency from consent to processing over his data within the framework of an order, if he wishes so. But also to be able to introduce criticism in order to be able to change previously defined conditions and thus flexibly meet the technical and moral change. Privacy is to be understood as a mediator of reciprocal sympathy and tolerance between data provider and data recipient, which can be implemented by means of a Privacy Language.**

Keywords*— *access, control, culture, data, ethic, freedom, GDPR, law, management, philosophy, privacy, protection, regulation, requirements, security, society, strategy, supervision

I. Introduction

Understood as a three-dimensional space of freedom, the world wide web (www), in a hidden fourth orientation, is home to a dimension of surveillance that endangers the basis of our society. A danger, due to the loss of trust in the www itself, created by an all-encompassing transparency of action and thus the impossibility to take on his role as a public person by means of intransparencies. The open society, a concept of Karl Popper from 'The Open Society and its Enemies' [23] of 1945, is often equated in the public debate with words such as liberalism, democracy, arbitrariness, market economy or laissez-faire and, in the sense of the inventor, is, however, supposed to be a kind of toolbox for freedom.

Does privacy, for example, fit into this box of handicrafts in order to hide the fourth dimension of surveillance and thus create a new area of freedom?

II. Ethical Considerations on Open Society according to Popper for a Social, Digitally Transformed Data Culture

A. Freedom and fear

According to Erich Fromm, who wrote about the open society shortly before Popper´s published argument, we are afraid of freedom [16]. Fromm, in his remarks, distinguishes between three fear-driven reactions to freedom. On the one hand the compulsion to conformism, on the other hand the voluntary submission of the autocracies as well as the tendency to self-damage, in which everyone does what he or she wants, in each case at the expense of others. On the basis of the correctness of this assumption, the equal representation in the social networks, the exposing of the self as currency for digital consumer goods or the culture of unbridled hate speech could be seen in a context of fear of the space of freedom. Poppers' open society [23] is now to show a fourth way, which can be taken as a reaction to freedom, without any traits of fear. Before this, it would have to be clarified whether privacy, a fear-driven human reaction to freedom, or a component of the fourth path is Poppers' social philosophy, which understands to use privacy as an instrument against the fear of freedom.

B. Privacy and fear

If privacy were to be used as a factor in the opposing product of a closed society in order to reduce complexity, this would be an attempt to provide security that the open society cannot provide. This would subject us to a control illusion that suggests that we could live in a world that is objectively insecure, with the feeling of being safe through privacy. As a fear-driven reaction to freedom, privacy thus merely offers a supposed security that closes one's eyes so as not to have to see and acknowledge what exists. This is one of the most important statements of Karl Poppers' social philosophy that we have to learn - to deal with uncertainties. To this end, we as a society should define a non-negotiable ground for all that we do not want and create what we want against a lid. The protection of our data as a firmly anchored ground of privacy and data security, or as a lid of data transparency and extensive use, offers two opposing poles, which it can be at hand as a tool for freedom. An emerging naive luxury of contempt for data ethics would be reduced to absurdity by a fourth way of seeing, accepting and processing uncertainty.

C. Negative utilitarianism

What increases the prosperity of society, we, in the form of a negative utilitarianism according to Popper, cannot determine as society, but only individually. The individual possible actors at the forefront of privacy in a digital representation are distributed among several individuals who are empowered to make decisions about the handling of millions or even billions of dollars of data they receive. Possible influencers may include clients, designers, developers and software architects as well as application operators or providers of integrated program lines.

III. Privacy Status

A. Privacy guidelines

In order to be recognized as a benchmark, data ethics guidelines in the form of privacy must be created by the autonomous individual, which in turn must also protect the autonomous individual. Whether described as data protection, privacy or privacy protection, guard rails in the form of laws, as a guideline for possible influencers, have produced an extremely large number of texts in the last 50 years [22]. These guard rails are intended to reflect moral standards by

978-1-7281-2856-6/19/$31.00 ©2019 IEEEE

agreeing on a common legal text, which has also been successful. But what these individual regulations mean and how they are to be interpreted remains controversial. Just as with the concept of freedom, the 'object of the free act' [24] also decides with regard to privacy whether freedom or privacy is 'good or bad, should really be or not' [24]. As an act of state security, eavesdropping thus acquires legitimacy for unrestricted data transparency, which is flushed through the network by means of fibre-optic cables. At the same time, the role of an individual on the www is recorded, stored and analysed by economic platform oligarchs.

B. *Privacy classification*

When privacy is regarded as a protected good, it is home to a wealth of ramifications. A rough first classification of this good can take place in individual needs, interests of the individual and social constructions as well as social or structural characteristics. If the branch of individual aspects is examined more closely, concepts such as confidentiality, property, freedom of decision or even personality development come to light. When considering social objects of protection, concepts such as human dignity, communication protection, information order or the maintenance of the functional differentiation of society come also to light. This abundance of ramifications characterizes the processes of the digital in particular. In order to obtain a coherent picture of a role of an individual, a process or a pattern, snapshots of a single date are not sufficient [22]. The mapping of processes through the transparency of entities, relationships and weightings is needed.

IV. Challenge of Privacy

A. *Privacy and the Privacy Paradox*

Privacy has many facets which have to be considered for supporting a holistic management approach. The user, as the source of personal data, expresses his concerns about his personal data processing. But as detailed by the Privacy Paradox [25] [6] [19] [5], users are, generally speaking, not willing to put additional effort into the protection of their privacy. Thus, they have to be protected by default which is realized in the EU by the legal framework GDPR. This protection comprises transparent information on the processing of the personal data and control due to strengthened rights, which are expressed and regulated within the privacy policy. Both transparency and control over the processing of personal data are the main challenges.

Transparency is a challenging task as privacy policies are commonly presented as legal text which makes them hard to comprehend and hard to be consulted by the user. To enable transparency, privacy languages have not only to be machine-readable but also human-readable. The second issue is how to efficiently enforce the users' control over personal data. Besides legal policies express the handling of personal data, no technical measures for preserving privacy are directly bound to such policies.

Therefore, the user can only trust the company to process the personal data only for the defined purposes. But this is also an issue for companies, which intend to comply with the legal framework for which they are responsible. The processing of personal data according to the privacy policy is hereby a core challenge which has further aspects to be considered. Efficient processing of personal data is essential for companies. On the one hand, this requires the preservation of privacy according to the agreed on privacy policies of individuals. On the other hand, the utility of the data-set has to be preserved such that the data is still useful for the intended purpose. Thus, a trade-off between privacy and utility has to be considered. Moreover, user requests regarding their Data Subject Rights have to be supported by technical means to support the privacy officer in his task. The gap between legal requirements and their technical realization using privacy-preserving technologies is due to the lack of a machine-readable representation of privacy policies.

B. *Privacy with Communication Privacy Management (CPM) theory*

The core structure of a privacy policy is not only specific to the GDPR, but a generic description of privacy rules based upon the upon the individuals' perception of privacy. Privacy is perceived by individuals as a time and space in which they can be autonomous and have a limited and protected communication [28]. Hereby, privacy is interpreted as the dynamic process which gives or limits access to (personal) information with the goal to achieve balance between actual and desired privacy [3]. This interpretation of privacy has been extended by Petronio [20] with its Communication Privacy Management (CPM) theory.

The CPM theory states that privacy is a range of complete openness to complete closeness, which is regulated by people via a dialectic approach. Initially personal information is owned by the individual (data source) itself, but it can be shared and distributed to others (data recipients) such that the ownership is distributed to many [11] [12]. If ones' privacy is violated, then corresponding privacy rules are adopted by the individual, e.g., information is no longer shared with specific individuals [11] [12]. Therefore, core elements of a privacy policy can be matched to the perceived privacy according to the CPM theory.

C. *Privacy with purpose based access control*

Considering the before mentioned Communication Privacy Management (CPM) theory, which states that privacy is perceived as a range from complete openness to complete closeness [20], mechanisms for controlling who has access to personal data have to be incorporated in a privacy language. Access control mechanisms allow exactly this, thus the requirement states that:

- A privacy language has to enable purpose-based access control.
- A privacy language should hereby consider both the source, e.g., a user, and the recipient, e.g., a company, as identifiable entities.

The data flow should be hereby controllable between any combinations of such entities, e.g., user and company, user and user, or company and company. Furthermore, access to personal data should be purpose specific, e.g., a company can use the phone-number of Bob for emergency contacts but not for advertisement. Therefore, fine-grained access control is required for authenticating and authorizing the requesting entity to access personal data.

Similar problem statements have been worked on various other domains, e.g., privacy policies for mobile devices [9], access control in cloud [26] and IoT [15] [29] environments.

GDPR requires a purpose-based processing of personal information [17], thus a differentiation is necessary. This has

been addressed for relational databases [10]. Especially in the domain of health care, in which very sensitive and private information is stored and processed, purpose-based access control mechanisms are required. Therefore, hippocratic database systems have been proposed [2] [7], which goal is to enable privacy [18]. Privacy meta-data, which could be expressed using a privacy language, is hereby utilized to strengthen the access constraints to the data [1].

D. Privacy with Privacy Languages

The processing of personal information is omnipresent in our datadriven society enabling personalized services, which are regulated by privacy policies. Although privacy policies are strictly defined by the General Privacy Regulation (GDPR), no systematic mechanism is in place to enforce them. Especially if data is merged from several sources into a data-set with different privacy policies associated, the management and compliance to all privacy requirements is challenging during the processing of the data-set. Privacy policies can vary hereby due to different policies for each source or personalization of privacy policies by individual users. Thus, the risk for negligent or malicious processing of personal data due to defiance of privacy policies exists.

To tackle this challenge, a privacy-preserving framework is proposed. Within this framework privacy policies are expressed in the proposed Layered Privacy Language (LPL) [14] which allows to specify legal privacy policies and privacy-preserving de-identification methods. The policies are enforced by a Policy-based De-identification (PD) process [13]. The PD process enables efficient compliance to various privacy policies simultaneously while applying pseudonymization, personal privacy anonymization and privacy models for de-identification of the data-set. Thus, the privacy requirements of each individual privacy policy are enforced filling the gap between legal privacy policies and their technical enforcement.

V. Trilemma of open Society

A life can be coped with shaped by processes, an order of digitalization, in a world that is always incomplete due to its complexity, only by balancing Poppers' trilemma of open society [23] - order, freedom and criticism.

A. Order

Complex worlds cannot offer order in the sense of controllability, operability or even control. Due to their incomprehensible structures, levels and dimensions, they always remain both incomplete and intransparent. On the one hand, this gives complexities their charm and, on the other, an uncompensable lack of security. According to Brunnhuber [8], it would be a sign of humility to acknowledge that we cannot fully control or oversee complex digitalities. As humility in the sense of courageous service, the question arises as to whom we should be courageously committed to service. Obligation towards the creators of the www, to the developers of algorithms, perhaps to the beneficiaries of the Net? Or obligation even towards artificial intelligences, which control, expand and further develop branches of processes?

The basis of the complex worlds of artificial intelligences are information architectures whose order, despite humility, 'must not amount to undemocratic control models, neither consumer-driven leadership by tech corporations nor the supervising version of governments' [27].

However, a rough order in the sense of basic understanding offers a possible approach to complexities. 'Empathy is not equal to data transmission' [27] because human reason is not based solely on rationality. Thus, there would be a possibility to open up the completely incomprehensible world, in its basic features, by means of emotions, through a way of thinking that is far removed from reason. Through more observation, analysis and feedback, this feeling could be trained and optimised in order to develop an intuitive approach to the www, accompanied by security.

A further element for understanding the complex world is reciprocal ambivalence. This means a mutual tolerance, in which not everyone is forced to take the other's opinion and yet fights for the freedom of the other to be allowed to say his opinion in the future, with the accompanying ability to endure contradictions, polarities and opposites and to draw a gain in knowledge from these contradictions. An insight should be gained that changes and expands one's own system of order.

B. Critique

Not in the sense of dialectic, the second aspect of Poppers' Trilemmas is thought of as critique, but as a capacity for differentiation, which presupposes freedom of choice. A critique, of being able to separate and not of nagging, is desired, which applies truth as a yardstick for quality. The possibility of criticism as freedom of opinion, as guarantor for transparency and criterion of change through a constant implementation of criticism. Thus critique interlocks with order, in which transparency and change fuel the understanding that forces complexity into new, more manageable structures. Such structures can be created, for example, through privacy policies, which thereby promote understanding and facilitate transparency. The freedom of choice for expressing, accepting and implementing criticism sets its standard both on the truth and on the individual's discretion as to the relevance of what is said. Since complexity does not claim to be complete, there is also no possibility of complete transparency, which in turn favors uncertainties.

C. Freedom

Freedom also includes the mechanism that makes it possible to escape. A deselectability but also a right to ignorance or a right to free riding, i.e. a right to use default settings must be provided in a free area. In an implementation considered policies or privacy systems enable an integration of privacy by default, which GDPR already presides over as a paradigm. Thus a freedom 'must not lose its right vis-à-vis other creative freedoms and powers in the very moment in which it chooses the morally bad and non-be-should-be' [24]. At the same time, it is subject to the danger of becoming accustomed and of considering it as a matter of course. Hannah Arendt [4] wrote, 'That we then realize our human being when we act politically. Then we are free. Then we are man'. The problem of freedom lies in the fact that man cannot be forced to act politically, it must come out of the self. However, a spark of hope and a pinch of confidence is enough to spark commitment in people. If this inflammation does not succeed in humans however, justified pessimism and resignation threaten by unfreedom.

VI. Summary with Privacy in Trilemma of open Society

The question was posed as to the accuracy of fit of the privacy instruments in the Poppers' toolbox of freedom in order to hide the fourth dimension of surveillance in favour of a social-digital data culture.

Starting from the assumption that data protection is based on the trilemma of open society after Popper, it would also be a multi-tool against the fear of freedom and thus also a tool for adopting complexity in the digital world. Data protection then provides a kind of magnifying glass for transparency and the subsequent feeling of security, which implies that the protection to be created would provide a minimum level of knowledge against the attack scenarios that arise. At the same time, data protection served as a structural provider for frameworks and patterns, for the possibility of a meta-view to establish a basic order, which as a guardrail flexibly meets technical and moral change. The protection of data as an acceptor of criticism and guarantor of the constant development and advancement of the digital society. As well as the tool of data protection as a kind of glue for the connection of reciprocal sympathy and tolerance between data provider and data recipient.

REFERENCES

[1] R. Agrawal, P. Bird, T. Grandison, J. Kiernan, S. Logan, and W. Rjaibi. 'Extending relational database systems to automatically enforce privacy policies." In: 21st International Conference on Data Engineering (ICDE'05). Apr. 2005, pp. 1013–1022. doi: 10. 1109/ICDE.2005.64.

[2] Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. 'Hippocratic databases." In: VLDB'02: Proceedings of the 28th International Conference on Very Large Databases. Elsevier. 2002, pp. 143–154.

[3] Irwin Altman. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. Monterey, Calif. : Brooks/Cole Pub. Co., 1975.

[4] Hannah Arendt. Freedom and Politics: A Lecture In: Chicago Review Vol. 14, No. 1 (SPRING 1960), pp. 28-46.

[5] Susan B. Barnes. "A privacy paradox: Social networking in the United States." In: First Monday 11.9 (2006). issn: 13960466. doi: 10.5210/fm.v11i9.1394. url: https://firstmonday.org/ojs/index.php/fm/article/view/1394.

[6] Susanne Barth and Menno DT De Jong. "The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review." In: Telematics and Informatics 34.7 (2017), pp. 1038–1058.

[7] R. Bhatia, and M. Singh. 'Preserving Privacy in Healthcare Web Services Paradigm Through Hippocratic Databases." In: IntelligentComputing,CommunicationandDevices.Ed.byLakhmi C. Jain, Srikanta Patnaik, and Nikhil Ichalkaranje. New Delhi: Springer India, 2015, pp. 177–188. isbn: 978-81-322-2012-1.

[8] Stefan Brunnhuber (2019). The open society. A plea for freedom and order in the 21st century. Munich: oekom Publishers.

[9] S. Bugiel, S. Heuser, and A. Sadeghi.'FlexibleandFine-grained Mandatory Access Control on Android for Diverse Security and Privacy Policies." In: Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13). Washington, D.C.: USENIX, 2013, pp. 131–146. isbn: 978-1-931971-03-4.

[10] Ji-Won Byun, Elisa Bertino, and Ninghui Li. 'Purpose Based Access Control of Complex Data for Privacy Protection." In: ProceedingsoftheTenthACMSymposiumonAccessControlModels and Technologies. SACMAT '05. New York, NY, USA: ACM, 2005, pp. 102–110. isbn: 1-59593-045-0. doi: 10.1145/1063979. 1063998.

[11] Jeffrey T Child, and David A Westermann. 'Let's be Facebook friends: Exploring parental Facebook friend requests from a communication privacy management (CPM) perspective." In: Journal of Family Communication 13.1 (2013), pp. 46–59.

[12] Jeffrey T Child, and Sandra Petronio.'Unpackingtheparadoxes of privacy in CMC relationships: The challenges of blogging and relational communication on the www." In: Computermediated communication in personal relationships (2011), pp. 21– 40.

[13] A. Gerl, and S. Becher. Policy-Based De-Identification Test Framework 2019 IEEE World Congress on Services (SERVICES), 2019 , 2642-939X , 356-357.

[14] A. Gerl; N. Bennani; H. Kosch, and L. Brunie, A. Hameurlain, and R. Wagner (Eds.) LPL, Towards a GDPR-Compliant Privacy Language: Formal Definition and Usage Springer-Verlag GmbH Germany, part of Springer Nature 2018, 2018 , Transactions on Large-Scale Databases and Knowledge-Centered Systems (TLDKS) , pp. 1-40.

[15] Kai Fan, Huiyue Xu, Longxiang Gao, Hui Li, and Yintang Yang. 'Efficient and privacy preserving access control scheme for fog-enabled IoT." In: Future Generation Computer Systems 99 (2019), pp. 134 –142. issn: 0167-739X. doi: 10.1016/j.future. 2019.04.003.

[16] Erich Fromm. The fear of freedom. London: Paul, Trench, Trubner & Co (International library of sociology and social reconstruction), 1945.

[17] General Data Protection Regulation. Regulation (EU) 2016 of the European Parliament and of the Council of 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. Apr. 2016. url: http://data.europa.eu/ eli/reg/2016/679/oj.

[18] Tyrone Grandison, and Kristen LeFevre. 'Hippocratic Database." In: Encyclopedia of Cryptography and Security. Ed. by Henk C. A. van Tilborg and Sushil Jajodia. Boston, MA: Springer US, 2011, pp. 556–559. isbn: 978-1-4419-5906-5. doi: 10.1007/978-1-4419-5906-5_679.

[19] Adam N. Joinson, Ulf-Dietrich Reips, Tom Buchanan, and Carina B Paine Schofield. "Privacy, trust, and self-disclosure online." In: Human–Computer Interaction 25.1 (2010), pp. 1–24.

[20] S. Petronio. Boundaries of Privacy: Dialectics of Disclosure. SUNY series in communication studies. Albany, NY: State University of New York Press, 2002. isbn: 0-7914-5515-7.

[21] Sandra Petronio, and Jennifer Reierson. 'Regulating the privacy ofconfidentiality:Graspingthecomplexitiesthroughcommunication privacy management theory." In: Uncertainty, information management, and disclosure decisions: Theories and applications (2009), pp. 365–383.

[22] Jörg Pohle. Data protection and technology design. History and theory of data protection from an informatics perspective and implications for technology design. Dissertation. Humboldt-Universität zu Berlin, 2016. Berlin.

[23] Karl R. Popper. The open society and its enemies. 7th ed. Tübingen: J.C.B. Mohr Publishers, 1992.

[24] Karl Rahner. Freedom and Manipulation in Society and Church. 2nd ed.,: Kösel (Munich Academic Publications, vol. 54), 1971. p. 9.

[25] Irina Shklovski, Scott D Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. "Leakiness and creepiness in app space: Perceptions of privacy and mobile app use." In: Proceedings of the 32nd annual ACM conference on Human factors in computing systems. ACM. 2014, pp. 2347–2356.

[26] S. Ruj, M. Stojmenovic and A. Nayak. 'Privacy Preserving Access Control with Authentication for Securing Data in Clouds." In: 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012). May 2012, pp. 556–563. doi: 10.1109/CCGrid.2012.92.

[27] Leon R. Tsvasman. AI Thinking. Dialogue of a thought leader and a practitioner on the meaning of artificial intelligence. Baden-Baden: Ergon publishing house, 2019. pp. 80-91.

[28] Alan F. Westin. 'Privacy and Freedom." In: Atheneum Press (1967)

[29] Yang Yang, Xianghan Zheng, Wenzhong Guo, Ximeng Liu, and Victor Chang. 'Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system." In: Information Sciences 479 (2019), pp. 567 –592. issn: 00200255. doi: https://doi.org/10.1016/j.ins.2018.02.005. url: http://www.sciencedirect.com/science/article/pii/S0020025518300860.