H. Roßnagel et. al. (Eds.): Open Identity Summit 2019,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019 71

Anonymization Is Dead – Long Live Privacy

Jan Zibuschka[1], Sebastian Kurowski[2], Heiko Roßnagel[2], Christian H. Schunck[2], and Christian Zimmermann[1]

Abstract: Privacy is a multi-faceted, interdisciplinary concept, with varying meaning to different people and disciplines. To most researchers, anonymity is the "holy grail" of privacy research, as it suggests that it may be possible to avoid personal information altogether. However, time and time again, anonymization has been shown to be infeasible. Even de-facto anonymity is hardly achievable using state-of-the-art cryptographic anonymization techniques. Furthermore, as there are inherent tensions between the privacy protection goals of confidentiality, availability, integrity, transparency, intervenability and unlinkability, failed attempts to achieve full anonymization may make it impossible to provide data-subjects with transparency and intervenability. This is highly problematic as such mechanisms are required by regulation such as the General Data Protection Regulation (GDPR). Therefore, we argue for a paradigm shift away from anonymization towards transparency, accountability, and intervenability.

Keywords: privacy; anonymization; identity management; accountability; transparency

1 Introduction

Privacy is an interdisciplinary concept. It is considered to be a basic human right in contemporary democracies [Pa10], hinting at a legal provenance. At the same time, it is also determined by the technology used to process personal information, making it an issue of information technology in addition to regulation [TBC15]. It can also be looked at as something that is valued by individuals, making it amenable to economic investigation [Pa10], and relevant to the development of societies, leading to sociological investigation of the concept [Ba12].

Privacy is also polysemic; it may mean different things to different people [Ba12]. However, at least as far as the technological facet of privacy is concerned, in recent years there has been considerable progress towards a standard model of privacy: the protection goals for privacy engineering [HJR15] that form the basis of the standard data protection model [We18]. These protection goals comprise the industry standard protection goals for cyber security (i.e. the "CIA" triad of Confidentiality, Integrity, and Availability) [vSvN13], and extend them by protection goals specific to privacy (i.e. transparency, intervenability, and unlinkability). It should be noted that the privacy

[1] Robert Bosch GmbH, Zentralbereich Forschung und Vorausentwicklung, Renningen, 70465 Stuttgart, Deutschland; [jan.zibuschka] / [christian.zimmermann3] @de.bosch.com
[2] Fraunhofer IAO, Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO, Competence Team Identity Management, Allmandring 35, 70569 Stuttgart, Deutschland; [sebastian.kurowski] / [heiko.rossnagel] / [christian.schunck] @iao.fraunhofer.de

protection goals – as the GDPR - thus address both the right to data protection and the right to privacy in the EU Charter of Fundamental Rights.

Of those privacy-specific goals, it seems that confidentiality and unlinkability (with anonymity as one of its facets) have received the most attention in research. This is also reflected in earlier works of some of the authors of the new protection goals, which differentiate anonymity, unlinkability, undetectability, unobservability, and pseudonymity as top level protection goals [PH10]. Of these facets of unlinkability, anonymization, i.e., entirely removing the linkability of a piece of information to an individual, while retaining at least some of the utility for which the information was collected in the first place [PPC17], has been identified as the gold standard [BMS13].

However, full anonymization, making it theoretically impossible to link personal information to an individual, has been shown to be impossible to implement in many cases due to leakage [DT13]. Even de-facto anonymization, making it infeasible to link personal information to an individual with reasonable effort, is hardly achievable with state-of-the-art cryptographic techniques, although it has been in the focus of research for the last ten years [Sh10, PPC17, BMS13]. At the same time, de-anonymization techniques are continually evolving, and routinely identify upwards of eighty percent of individuals in datasets with very sparse information [Ji14]. In this paper, we argue that this enduring failure to anonymize individual information has fundamental consequences for privacy engineering and that we need a paradigm shift away from anonymization towards focussing more on transparency, accountability and intervenability.

The rest of the paper is structured as follows. We first look at the research trends of privacy in the last two decades, which show a strong emphasis on confidentiality and unlinkability (mostly in its facet of anonymity). In section 3 we argue that solely relying on anonymization techniques is a flawed approach that often leads to undesired results. In section 4 we propose a paradigm shift towards transparency, accountability and intervenability. Section 5 concludes our findings.

2 Research trends

To obtain some insight into recent trends in privacy research we used the Elsevier Scopus service to study which of the privacy protection goals of [HJR15] and selected other keywords are mentioned explicitly together with the word “privacy” in title, abstract, and keywords of publications listed in Scopus since the year 2000.

This approach is naturally very coarse-grained as privacy protection goals may still be addressed explicitly in the full text of a paper. The six keywords of the protection goals could further be mentioned in a context other than the one implied by the protection goals. However, for getting an indication of research trends and the emphasis put on different aspects of privacy research, this approach can serve as a first step. A more detailed study would require a review of thousands of abstracts and publications, which

is beyond the scope of this paper.

The results of our analysis are shown in Figure 1. Among the privacy protection goals, the CIA triad is clearly in the lead. In 2017, 802 papers mention confidentiality, 482 integrity, and 337 availability together with privacy (note, that papers are counted separately in each category, e.g. in 2017 161 mention both confidentiality and integrity, and 37 papers confidentiality, integrity and availability). Clearly under-represented are transparency, unlinkability and intervenability with 158, 38 and 1 papers published in 2017, respectively.

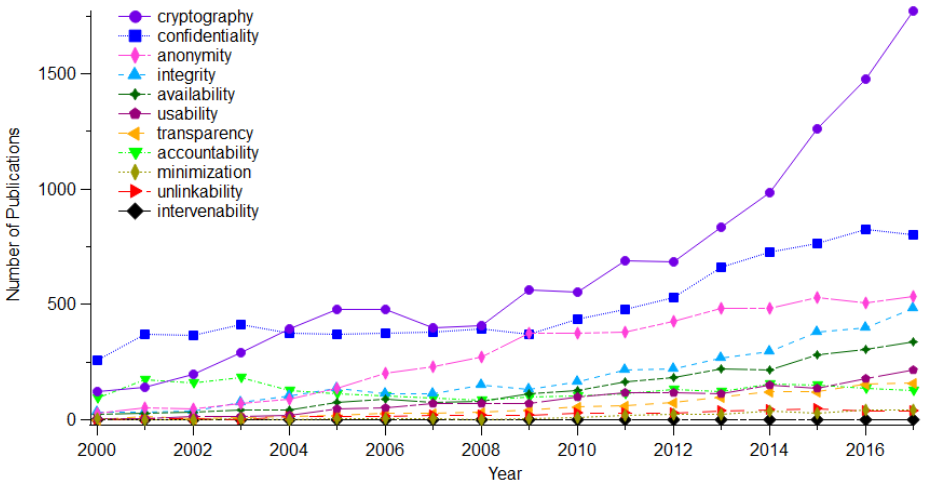

Fig. 1: Number of Scopus Publications per year with "privacy AND keyword" in title, abstract or keywords

Beyond the protection goals, several other keywords deserve particular attention:

- Anonymity as a facet of unlinkability
- Usability
- Accountability ("The controller shall be responsible for, and be able to demonstrate compliance" GDPR Article 5(2) which often receives less attention than Article 5(1)[3])

In 2017, 534 papers refer to anonymity, 217 to usability and 128 to accountability. This promotes anonymity to be a keyword mentioned in frequency second only to confidentiality.

However, the number of appearances of all other keywords discussed is vanishingly small compared to the appearance of "cryptography" in title, abstract and keywords of

[3] https://www.consultancy.uk/news/13487/six-privacy-principles-for-general-data-protection-regulation-compliance

1772 papers in 2017. In fact, just the rise in papers mentioning cryptography between 2016 and 2017 is larger than the number of papers referring to each one of the key words transparency, unlinkability, intervenability, accountability, or usability in the same year.

Overall this analysis indicates that privacy research has a strong trend towards solutions and concepts that are based on cryptography and those aspects that can be achieved (to a significant extend) by cryptographic means including anonymity and the privacy protection goals of confidentiality and integrity (see Figure 2).

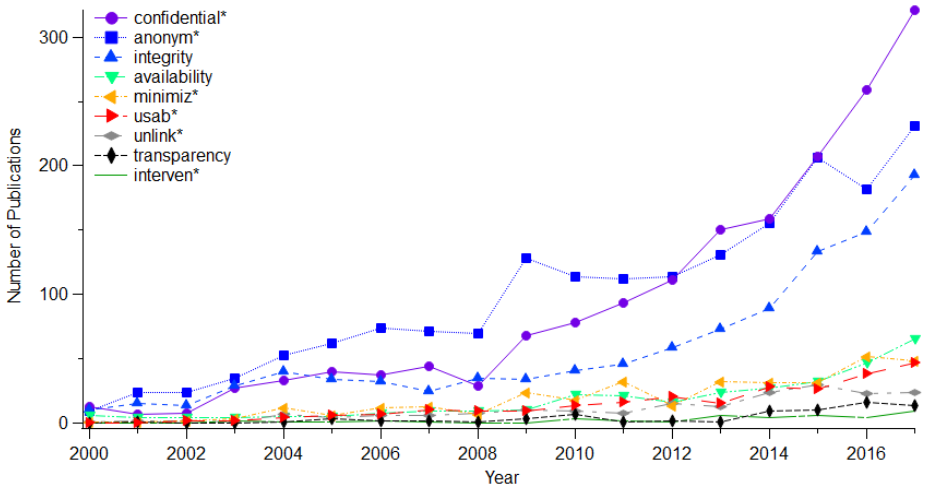

Fig. 2: Number of Scopus publications per year with "privacy AND crypto*AND keyword" (see figure) in title, abstract or keywords.

To substantiate our observations we have also analyzed the 49 papers contained in the replication set of a recent review of privacy patterns [LFH17]. These papers have a focus on integrating privacy concerns in software engineering and should thus address hands-on challenges arising when developing software with a privacy impact.

Three reviewers (who are among the authors) independently analyzed title and abstract of these papers with the goal to identify which privacy protection goals [HJR15] are addressed. Each contribution was coded with one or multiple privacy protection goals [HJR15]. Each reviewer coded the contributions independently. Codings were discussed afterwards, the agreements and disagreements were counted and the inter-coder reliability (IRR) was computed [MH94]. At 95.6%, the IRR was very high, showing strong agreements between the codes of the reviewers. Within each code, the IRR was above 90% (Tab. 1). However, 20 of the 49 papers could not be coded based on abstract and title and were therefore not included in the analysis.

Code	Confidentiality	Transparency	Intervenability	Availability	Unlinkability	Integrity
#	16/18/19	9/8	3/2/4	0	17/19	4/5
IRR	93.88%	97.96%	95.92%	100%	91.84%	93.88%

Tab. 1: Coded appearances of protection goals in privacy literature sample

Confidentiality was identified in 16 – 19 contributions, along with unlinkability in 17 – 19 contributions (depending on the reviewer) followed by transparency, integrity and intervenability. Note that in this analysis the reviewers treated anonymity as a facet of unlinkability and thus included papers addressing anonymity under the label unlinkability. Finally, no contributions could be attributed to focus on availability. Very notably, trends similar to the Scopus search emerge, even though the sample used is focused on software development and thus on a rather pragmatic approach towards privacy. However, the number of contributions that focus on transparency stands out as the third most frequent topic. A closer look shows that most papers related to "transparency" concentrate on the clarity of privacy policies, informed consent, notifications, and privacy assessments rather than transparency in data and meta-data processing.

Overall the protection goals of confidentiality and anonymity (unlinkability) dominate the discourse while other protection goals like intervenability, availability, integrity and transparency are under-represented. Addressing the under-represented privacy protection goals appropriately requires non-trivial organizational and technological solutions, but comparatively little research is apparently carried out in these directions.

3 The Anonymization Fallacy

This situation would be acceptable if anonymity was achieved in most use-cases. For example, the GDPR is not applicable to anonymous data and, thus, there is no need to address the privacy protection goals of transparency, intervenabilty, and accountability if personal data is properly anonymized. Anonymization implies that data which previously pointed to individuals is processed and afterwards cannot be uniquely related to these individuals anymore.

When automated data processing first became available, anonymization of personal information was considered quite the trivial task: just remove the person's name or social security number. This, however, did not work, since the data stayed relatable to a person by inference and profiling. The unexpected complexity of anonymization led to situations where organizations stored, and even published, data they believed was anonymous, but which in fact was quite easy to de-anonymize [Oh09].

This does not necessarily apply to aggregated data: It is quite easy to see that providing results of a statistical analysis of large datasets in an anonymous way is trivial: whether an individual suffers from a specific illness is critical personal information, however, the percentage of the overall population of Europe suffering from the same illness is not.

In contrast, anonymization of individual information has proven far more elusive, even though various mechanisms have been proposed to this end. Those mechanisms range from simply removing personal identifiers such as the individual's name [Oh09] to sophisticated privacy-enhancing technologies based on, e.g., k-anonymity, l-diversity, t-closeness [LLV07], or differential privacy [BMS13]. It should be noted, however, that applying those technologies is a careful balancing act [Pa06], and the required trade-off between processing utility and privacy protection may very well fail and lead to either very limited protection [Sh10], or enormous distortion of even trivial calculations [BMS13]. At the same time, de-anonymization techniques are continually evolving, and routinely identify upwards of eighty percent of individuals in datasets with very sparse information [Ji14]. Further, according to literature, it is impossible to anonymize:

- Location information [ZB11, Kr07, Sh10]
- More generally, dynamic behavior [DT13]
- And any form of structured individual data in general [Ji14].

What makes this especially problematic is the polysemy of the term anonymity. While computer scientists commonly see anonymity as a relative concept, and have developed various metrics for determining the degree to which information has been anonymized [Ke08], to legal scholars and data protection practitioners anonymity signifies the absence of personal information, at least to a degree where it is not feasible to establish a link to any individual without disproportionate effort (de-facto anonymization). From a technical point of view, anything beyond de-facto anonymization cannot be reached, as some identifying information will be leaked in any case [DT13]. However, it is concerning that even the most advanced privacy-enhancing technologies for anonymization either leave a significant amount of individuals unprotected or entirely negate the utility of the processing [BMS13].

Hence, it appears questionable whether even de-facto anonymization is really achievable. Certainly, all investigations of its effectiveness indicate that it is not. In fact, accounts dating back as far as the seventies state that anonymization of individual information is impossible [Ja73]. This failure of anonymization is reflected in many practical applications. For example, Google street view links at least part of its pixelation efforts to user intervenability [Mi18], and the generated effect is limited, both with regard to coverage [Fr09] and with regard to effectiveness [Mi18], so we believe it should not be considered anonymization. Rather, anonymization attempts should be carried out with care, as unlinkability and intervenability are antipodal protection goals [HJR15], e.g. the unlinkability provided by pixelating an individual's face may prevent that individual from requesting deletion, while the remaining information (clothing,

location...) may be enough for an adversary to derive critical personal information. This may have very serious repercussions, such as sanctions under the European GDPR.

Therefore, if a significant part of research in the privacy space was concerned with relevance and applicability, we should observe a decrease in research covering anonymity, and an increase in investigations of pseudonymity. Despite the fact that pseudonymity was discussed in the early papers in privacy research e.g. [Ch81], and suggested as a suitable method for the legal structuring of IT security infrastructures [Ro95] more than 20 years before the GDPR, this certainly does not appear to be the case. In addition to what was discussed in Section 2, Fig. 3 shows the number of papers referring to "privacy AND anonym*" versus the ones that refer to "privacy AND pseudonym*"- a discrepancy that gives reason for concern.

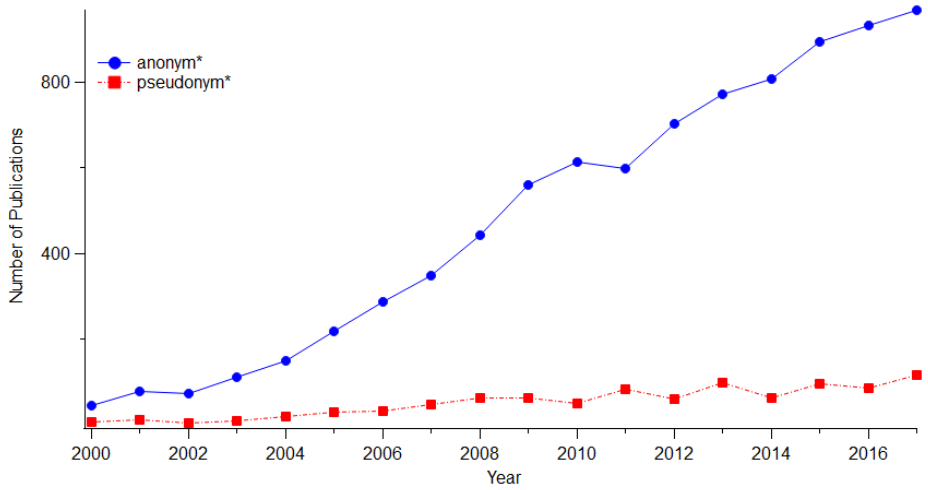

Fig. 3: Number of Scopus publications per year mentioning "privacy AND anonym*" or "privacy AND pseudonym*"

This paper thus takes the position that this enduring failure to anonymize individual information has fundamental consequences for privacy engineering. As processing insufficiently anonymized information may amount to processing personal information without taking the necessary precautions, specifically with regard to transparency and intervenability, a paradigm shift is needed. For any privacy-critical use case involving personal information, especially for commercial use cases emphasising compliance, we are convinced that research and development should move away from the focus on unlinkability and rather focus on transparency and accountability [ZC15] instead. This is especially pressing as recent application scenarios such as the social web, the sharing economy and the Internet of Things pose unprecedented challenges [VB18] for the implementation of measures for transparency and intervenability [LR13, To16], while at the same time, legislation such as Europe's GDPR foresees significant sanctions for negligence of transparency and accountability obligations [We18].

4 The Way Forward: Accountability

Above, we argued that anonymization is not a well-fitting approach to data protection. Furthermore, apart from very few cases such as statistical analysis of aggregated data, failed anonymization, i.e., anonymization that purportedly worked but did not actually remove linkability (either fully or de-facto), is in blatant contradiction to privacy goals such as intervenability. We believe that, in order to support informational self-determination and to not stifle beneficial processing of personal data, privacy engineering should focus on transparency, accountability, and intervenability instead of anonymization. But what exactly do we mean with "accountability" and how do we envision to enable it using technology?

Just like "privacy" the term "accountability" is multi-faceted and often seems to elude a clear definition. Notwithstanding, most definitions of accountability consider transparency and the possibility of sanctions constitutive elements of accountability [ZC15]. Further, control is often seen as a core dimension of accountability [Ko08] and, sometimes, accountability is even considered a form of control [Bo05].

As of late, accountability has also been explicitly postulated as an aspect of data protection in the GDPR, which defines its "accountability principle" in Article 5(2). In the GDPR context, the accountability principle refers to data controllers' obligation to not only adhere to the principles relating to processing of personal data defined in the regulation but to also be able to demonstrate compliance with those principles. Consequently, here, accountability refers to accountability of data controllers towards the regulator (and DPAs). As can be seen, the "accountability principle" postulated in the GDPR as an obligation to provide proof of compliance, also reflects the constitutive elements of accountability, i.e., transparency, sanctions and control or intervenability.

However, we consider accountability as defined in the GDPR with its focus on accountability regarding compliance and towards the regulator and supervisory authorities only one aspect of accountability as a privacy principle. While most certainly relevant and highly important, we argue that this notion of accountability needs to be complemented with user-centric accountability and respective technologies. In fact, studies have shown repeatedly that users face great difficulties in understanding and making privacy related choices [RDG17]. Obviously, users cannot on their own sanction a data controller, at least as long as one understands sanctioning in a narrow sense and does not consider boycotts or porting data to a different data controller as sanctions. Still, the GDPR already provides a broad set of instruments to support user-centric accountability and, in particular, its constitutive elements transparency and intervenability. For example, a data subject can exercise the rights to access and to object, rectification, restriction of processing and erasure in order to achieve transparency and intervenability, respectively (cf. Chapter 3 GDPR).

In order to exercise the aforementioned rights, the data subject must be unambiguously identifiable and, hence, her data cannot be anonymized. Further, exercising these rights

is often cumbersome, albeit the GDPR lays down several provisions aimed at facilitating exercise of these rights. Hence, we argue that research of technologies to support users to hold data controllers accountable needs to be intensified.

Technologically, we envision advanced transparency and intervenability measures, tackling the as of yet unsolved challenges of, e.g., IoT consent [LR13] and transparency mechanisms [To16]. Further, from a methodological perspective, privacy engineering methods need to be developed further to take into account the special characteristics of the Internet of Things and the shortcomings of anonymization. This must include not only the enhancement of methods for privacy impact assessment and ensuring privacy by design in general but also of methods and patterns for ensuring "transparency by design" and wide-ranging control capabilities for the user.

5 Conclusion

It is becoming increasingly clear that anonymization is quite easy to break, and even de-facto anonymization can hardly be reached for individual information. However, this does not need to be the end of privacy. To the contrary, it opens up new challenges for privacy research, as modern application scenarios make offering appropriate implementations of consent and transparency, which used to be quite trivial efforts, very challenging. We acknowledge that privacy-preserving (as opposed to privacy-enhancing) anonymous (as opposed to anonymizing) communication and credential technologies (cf. [Fö15]) are clearly working, and may even result in anonymity in use cases where no personal information was involved to begin with. We also acknowledge data minimization as a valid goal for privacy engineering, but we do point out that anonymization of individual personal information is an embodiment of an ideal that even technologists active in the cryptography space agree is unreachable [DT13].

In addition, we are convinced that the study of privacy in use cases where personal information is tied to a specific user is very relevant, and this relevance is only growing. Therefore, we encourage an emphasis on privacy research in transparency, accountability, and intervenability. The complexity of those topics in the aforementioned use cases is quite significant, and up till now, most experiments have been confined to platform operators such as Google [Or14], the operator of the street view service discussed above, who are clearly building knowledge about and fine-tuning their transparency and intervenability systems, such as the Google privacy dashboard [Or14]. After the broad failure of anonymization, with the proliferations of e.g. social networks, personal digital assistants, and the Internet of Things, and with the GDPR now binding, we can hardly afford an interregnum in privacy research where old methods are conserved without clear aim or merit. It would be regrettable if privacy researchers could not contribute to the pressing social questions raised by contemporary applications of technology.

Bibliography

[Ba12] Baghai, Katayoun: Privacy as a Human Right: A Sociological Theory. Sociology, 46(5):951–965, October 2012.

[BMS13] Bambauer, Jane; Muralidhar, Krishnamurty; Sarathy, Rathindra: Fool's Gold: An Illustrated Critique of Differential Privacy. Vanderbilt Journal of Entertainment and Technology Law, 16:701, 2013.

[Bo05] Bovens, Mark: Public Accountability. In (Ewan Ferlie, Laurence E. Lynn Jr., and Christopher Pollitt): The Oxford Handbook of Public Management, pp. 182-208, 2005.

[Ch81] Chaum. David L. Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM 24, 2 (February 1981), 84-90.

[DT13] Danezis, George; Troncoso, Carmela: You Cannot Hide for Long: De-anonymization of Real-world Dynamic Behaviour. In: Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society. WPES '13, ACM, New York, NY, USA, pp. 49–60, 2013.

[Fö15] Förster, David; Löhr, Hans; Zibuschka, Jan; Kargl, Frank: REWIRE – Revocation Without Resolution: A Privacy-Friendly Revocation Mechanism for Vehicular Ad-Hoc Networks. In: Trust and Trustworthy Computing. Springer, Cham, pp. 193–208, 2015.

[Fr09] Frome, A.; Cheung, G.; Abdulkader, A.; Zennaro, M.; Wu, B.; Bissacco, A.; Adam, H.; Neven, H.; Vincent, L.: Large-scale privacy protection in Google Street View. In: 2009 IEEE 12th International Conference on Computer Vision. pp. 2373–2380, 2009.

[HJR15] Hansen, M.; Jensen, M.; Rost, M.: Protection Goals for Privacy Engineering. In: 2015 IEEE Security and Privacy Workshops. pp. 159–166, 2015.

[Ja73] Jacobs, G.: Die Unwirksamkeit der Anonymisierung von Individualdaten — dargestellt am Beispiel der Amtlichen Studentenstatistik. Öff. Verw. Datenverarbeitung, 3:258–261, 1973.

[Ji14] Ji, Shouling; Li, Weiqing; Srivatsa, Mudhakar; Beyah, Raheem: Structural Data Deanonymization: Quantification, Practice, and Implications. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. CCS '14, ACM, New York, NY, USA, pp. 1040–1053, 2014.

[Ke08] Kelly, Douglas J.; Raines, Richard A.; Grimaila, Michael R.; Baldwin, Rusty O.; Mullins, Barry E.: A Survey of State-of-the-art in Anonymity Metrics. In: Proceedings of the 1st ACM Workshop on Network Data Anonymization. NDA '08, ACM, New York, NY, USA, pp. 31–40, 2008.

[Ko05] Koppell Jonathan: Pathologies of accountability: ICANN and the challenge of "multiple accountabilities disorder". Public administration review, 65(1):94-108, 2005

[Kr07] Krumm, John: Inference Attacks on Location Tracks. In: Pervasive Computing. Springer, Berlin, Heidelberg, pp. 127–143, 2007.

[LFH17] Lenhard, J.; Fritsch, L.; Herold, S.; A Literature Study on Privacy Patterns Research. In: 2017 43rd Euromicro Conference on Software Engineering and Advanced

Applications (SEAA), Vienna, 2017, pp. 194-201. doi: 10.1109/SEAA.2017.28

[LLV07] Li, N.; Li, T.; Venkatasubramanian, S.: t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. In: 2007 IEEE 23rd International Conference on Data Engineering. pp. 106–115, 2007.

[LR13] Luger, Ewa; Rodden, Tom: An Informed View on Consent for UbiComp. In: Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing. UbiComp '13, ACM, New York, NY, USA, pp. 529–538, 2013.

[MH94] Miles, M. B.; Huberman, A. M.: Qualitative Data Analysis: An Expanded Sourcebook. Sage Publications, Thousand Oaks, CA, 1994.

[Mi18] Minor, Jens: Google Maps: Bei Streetview verpixelte Gebäude werden in den Luftaufnahmen wieder sichtbar. GoogleWatchBlog, 2018. https://www.googlewatchblog. de/2018/02/google-maps-in-streetview/; acc. 2018-09-17.

[Oh09] Ohm, Paul: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, 57:1701, 2009.

[Or14] Ortlieb, Martin: The Anthropologist's View on Privacy. IEEE Security & Privacy, 12(3):85-87, 2014.

[Pa06] Pang, Ruoming; Allman, Mark; Paxson, Vern; Lee, Jason: The Devil and Packet Trace Anonymization. SIGCOMM Comput. Commun. Rev., 36(1):29–38, 2006.

[Pa10] Papacharissi, Zizi: Privacy as a luxury commodity. First Monday, 15(8), 2010.

[PH10] Pfitzmann, Andreas; Hansen, Marit: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, v0.34. 2010.

[PPC17] Pennarola, Ferdinando; Pistilli, Luca; Chau, Michael: Angels and Daemons: Is more Knowledge better than less Privacy? An Empirical Study on a K-anonymized openly available Dataset. In: ICIS 2017 Proceedings. AIS, Seoul, South Korea, 2017.

[Ra07] Radmacher, Mike; Zibuschka, Jan; Scherner, Tobias; Fritsch, Lothar; Rannenberg, Kai: Privatsphärenfreundliche topozentrische Dienste unter Berücksichtigung rechtlicher, technischer und wirtschaftlicher Restriktionen. In: 8. Internationale Tagung Wirtschaftsinformatik 2007 - Band 1. pp. 237–254, 2007.

[RDG17] Ramachandran, S.; Dimitri, A.; Galinium, M.; Tahir, M.; Ananth, I.V.; Schunck, C.; Talamo, M.: Understanding and granting android permissions: A user survey; In: Proceedings – 2017 International Carnahan Conference on Security Technology, Pages 1-6, 2017.

[Ro95] Roßnagel, Alexander. „Rechtliche Gestaltung informationstechnischer Sicherungsinfrastrukturen" in „Sicherungsinfrastrukturen: Gestaltungsvorschläge für Technik, Organisation und Recht" Hammer, (Editor), Springer-Verlag Berlin Heidelberg p. 177, 1995.

[RZ06] Roßnagel, Heiko; Zibuschka, Jan: Single Sign On mit Signaturen. Datenschutz und Datensicherheit - DuD, 30(12):773–777, 2006.

[Sh10] Shokri, Reza; Troncoso, Carmela; Diaz, Claudia; Freudiger, Julien; Hubaux, Jean-Pierre: Unraveling an Old Cloak: K-anonymity for Location Privacy. In: Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society. WPES '10, ACM, New York, NY, USA, pp. 115–118, 2010.

[TBC15] Tsormpatzoudi, Pagona; Berendt, Bettina; Coudert, Fanny: Privacy by Design: From Research and Policy to Practice – the Challenge of Multi-disciplinarity. In: Privacy Technologies and Policy. Springer, Cham, pp. 199–212, 2015.

[To16] Tolmie, Peter; Crabtree, Andy; Rodden, Tom; Colley, James; Luger, Ewa: "This Has to Be the Cats": Personal Data Legibility in Networked Sensing Systems. In: Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing. CSCW '16, ACM, New York, NY, USA, pp. 491–502, 2016.

[VB18] Voigt, Paul; Bussche, Axel von dem: Besondere Verarbeitungssituationen. In: EU-Datenschutz-Grundverordnung (DSGVO), pp. 311–320. Springer, Berlin, Heidelberg, 2018. DOI: 10.1007/978-3-662-56187-4_9.

[vSvN13] von Solms, Rossouw; van Niekerk, Johan: From information security to cyber security. Computers & Security, 38:97–102, 2013.

[We18] Weichert, Thilo: Datenschutz. In: Handbuch Staat, pp.1375-1385. Springer VS, Wiesbaden, 2018. DOI: 10.1007/978-3-658-20744-1_124.

[Wi12] Wicker, Stephen B.: The Loss of Location Privacy in the Cellular Age. Commun. ACM, 55(8):60–68, 2012.

[ZB11] Zang, Hui; Bolot, Jean: Anonymization of Location Data Does Not Work: A Large-scale Measurement Study. In: Proceedings of the 17th Annual International Conference on Mobile Computing and Networking. MobiCom '11, ACM, New York, NY, USA, pp. 145–156, 2011.

[ZC15] Zimmermann, Christian; Cabinakova, Johana: A Conceptualization of Accountability as a Privacy Principle. In: Business Information Systems Workshops. Springer, Cham, pp. 261–272, 2015.