Privacy as Enabler of Innovation

Daniel Bachlechner, Marc Van Lieshout, Tjerk Timan

Privacy as Enabler of Innovation

Daniel Bachlechner[1(✉)], Marc van Lieshout[2] and Tjerk Timan[3]

[1] Fraunhofer Institute for Systems and Innovation Research ISI, 76139 Karlsruhe, Germany and Fraunhofer Austria Research GmbH, 6112 Wattens, Austria
daniel.bachlechner@{isi.fraunhofer.de|fraunhofer.at}
[2] iHub – Interdisciplinary Research Centre on Security, Privacy and Data Governance, Radboud University, 6525 HT Nijmegen, The Netherlands
[3]Research Department on Strategy & Policy, TNO, 6525 GA Den Haag, The Netherlands

Abstract. Privacy has long been perceived as a hindrance to innovation. It has been considered to raise costs for data governance without providing real benefits. However, the attitude of various stakeholders towards the relationship between privacy and innovation has started to change. Privacy is increasingly embraced as an enabler of innovation, given that consumer trust is central for realising businesses with data-driven products and services. In addition to building trust by demonstrating accountability in the processing of personal data, companies are increasingly using tools to protect privacy, for example in the context of data storage and archiving. More and more companies are realising that they can benefit from a proactive approach to data protection. A growing number of tools for privacy protection, and the emergence of products and services that are inherently privacy friendly indicate that the market is about to change. In this paper, we first outline what "privacy as enabler of innovation" means and then present evidence for this position. Key challenges that need to be overcome on the way towards successful privacy markets include the lack of profitability of privacy-friendly offerings, conflicts with new and existing business models, low value attached to privacy by individuals, latent cultural specificities, skill gaps and regulatory loopholes.

Keywords: Privacy, Innovation, Data Protection, GDPR, Data Protection by Design, Fundamental Rights.

1 The role of privacy in innovation processes

Both in popular business and scholarly literature, the relationship between privacy and innovation is described in antagonistic terms. On the one side, evidence is presented for the detrimental consequences of having to deal with privacy in business processes, given the multitude of data sources, the various origins of these data sources and the problem of keeping track of the origins of data, let alone whether data has been collected on a legitimate basis in the first place. Hemerly, for instance, recalls the problems of having specific data be personal data [1]. Boats have an owner and as such identification numbers of boats belong to the category of personal data. This linkage prevents innovative research in identifying the impact of specific boats and vessels on fisheries.

A study by London Economics arrived at the conclusion that the introduction of the General Data Protection Regulation (GDPR) could amount to losses of 58 billon UK pounds due to failing businesses because of overtly mingling of privacy regulations with ordinary businesses [2]. Zarsky provides anecdotal evidence underscoring that a privacy-minded Europe has not been able to compete with a lesser privacy-minded USA in technology-related business innovations [3]. After having introduced five hypotheses that deal with the relationship between privacy and innovation, Zarsky uses the well-known innovation paradox to argue that the absence of clear leadership in Europe with respect to innovations based on information and communication technology (ICT) at least lends support to the statement that privacy has not led to a better position of Europe in this market. He pleads however for a nuanced view since it is very hard to convincingly demonstrate causality between different events (such as the stricter regime on privacy in Europe versus the higher rate of innovation in the USA) that are linked by a variety of factors.

On the other side, we can find utterances of business leaders who proclaim that adherence to privacy regulation results in a positive business case. One argument that can be heard is that the need to keep a register of data sources leads to greater transparency with respect to what data is kept for what purpose, amongst others resulting in less doubling of data and a stricter management of data sources within organisations [4]. A scarcely mentioned side-effect of cleaning up data is increased overall data quality, which makes data much more useful for the implementation of artificial intelligence (AI) applications [5]. Additionally, the increased need to encrypt data also contributes to greater security of data and fewer data breaches with high impact [6]. Finally, trust of consumers is enhanced when data policies are transparent, and consumers are kept informed and are asked for their consent [7].

Using different arguments and focusing on different points of view is nothing new. In reality, several of the arguments presented may be right at the same moment. So, while Europe has stricter privacy laws it still cannot be argued that this by itself will diminish the innovative capacity of Europe. We might argue, for instance, that these companies could rely upon a relatively friendly investment climate, with investors considering that investments in activities that promote current regulations is a promising investment. As we will see, however, the counter argument for this position has some truth in it as well: investors in the USA show more risk appetite and are willing to invest in specifically these kind of companies, i.e. in companies that within the USA might face a harder future than they might face in Europe but that still are able to blossom in the USA rather than in Europe just because of them being more risk prone.

Probably the most relevant driver for privacy as enabler of innovation is the institutional rearrangement that has taken place in the EU through the introduction of the GDPR. This regulation can be considered a turning point in the protection of persons with respect to the processing of their data [8]. For one, it introduces a strict accountability regime for controllers and processors. For another, its applicability overcomes the geographical limitation of "only" being relevant for the EU. Data subjects from places outside the EU still may rely on the same protective measures as inhabitants of an EU Member State, as long as these data subjects do business with companies that

are situated within the EU or are themselves in one of the EU Member States.[1] Data intensive companies that want to do business within the EU need to comply with the GDPR. This has already resulted in other countries and regions copying the approach of the GDPR in their own legislation.[2] The GDPR thus sets a number of clear indications concerning responsibilities of controllers and processors that – as we will demonstrate – paves the way for innovative approaches of dealing with personal data.

In this paper, we present an in-depth exploration of what precisely is at stake and outline ways forward. Section 2 starts by outlining the fundamental rights perspective that has become a common perspective on the relevance of privacy and data protection.[3] The section underscores the GDPR as the – temporary – outcome of a process that shows how the domain of privacy has been invaded by ICT. This invasion has led to a blurred distinction between privacy and data protection. When it comes to innovation, it is relevant to keep the focus on the interrelationship between privacy, data protection, and measures and tools that promote or hinder the development of new products and services. Section 3 deals with this topic and presents two takes on the rise and emergence of privacy markets. To that end, it outlines what should be understood by a privacy market. Section 4 continues with presenting additional empirical evidence for how privacy and innovation are interrelated focussing on key challenges and possible ways forward. Section 5, in the end, presents the conclusions that can be drawn on the basis of the presented insights and that form the present perspective on the emergence of a market for privacy.

2 Privacy and data protection – two sides of the coin

Privacy being a fundamental right was first acknowledged in the United Nations Declaration of Human Rights (1948). The Declaration was a response to the atrocities of the Second World War [10]. It referred to a famous speech of President Roosevelt in 1941 in which he phrased four freedoms that should be safeguarded, "the freedom of speech and expression, the freedom of worship, the freedom from want, and the freedom from fear" (quoted in Morsink [10]). Article 12 of the Declaration explicitly states the freedom from arbitrary interference with privacy, family, home or correspondence. Isaiah Berlin elaborated the concept of the freedoms in two directions: a negative free-

[1] Article 3 deals with the territorial scope of the GDPR. Contrary to its predecessor, Directive 95/46/EC, the GDPR is enforced as is it is in all EU Member States, thus enabling the indication of a territorial scope (which was absent in the previous Directive).

[2] Examples are the Data Protection Bill of Kenya (http://www.ict.go.ke/wp-content/uploads/2016/04/Kenya-Data-Protection-Bill-2018-14-08-2018.pdf; last accessed: 31/10/2019) and the Californian Consumer Privacy Act. The Kenyan Data Protection Bill is not yet accepted. The Californian Consumer Act has been passed in June 2018 [9].

[3] The phrase "data protection" may cause confusion, since it is not so much the data that needs protection but rather the person to whom these data refer. Because the term has become rather established, we will use it as well, keeping in mind that it should be read differently (namely: the protection of persons with respect to the processing of their data).

dom or the absence of coercion that should safeguard civilians from arbitrary interference by public authorities in their activities and a positive freedom or self-mastery that should enable citizens to develop themselves as autonomous persons in self-chosen directions [11]. While this perspective focuses specifically on the individual dimension of privacy, privacy has a collective, a group and a public dimension as well [12, 13]. The freedom of communication refers to the interaction between two or more persons, leveraging privacy above a merely individual level. Some have also referred to the need for safeguarding the freedom of association, which refers to the group dimension of privacy [14]. The impact of ICT on all these dimensions of privacy can be demonstrated in a rather straightforward manner. Interestingly, these days both public and private actors have considerable possibilities to infringe upon the privacy of individuals. Reference to the data crunchers that collect personal data in a large variety of different ways is sufficient to demonstrate that individual freedoms may be at stake in light of the business practices that these companies are deploying.[4] Official surveillance programmes go alongside with secret snooping and snuffing in personal data, and new ways of getting a foot in the private homes of families by voice recognition techniques such as Amazon's Alexa, Apple's Siri and Google Home, or collecting DNA samples [17, 18].

Still we can safely conclude that privacy is far from dead, notwithstanding the remark by Scott McNealy, then CEO of Sun Microsystems, made twenty years ago, of the opposite point of view[5]. Despite popular utterings of privacy being dead (meaning, privacy as a social value), privacy as a right, at least in Europe, is firmly embedded in constitutions [[19]]. Taking the Netherlands as an example, privacy is safeguarded in four consecutive articles in the Dutch constitution: article 10, 11, 12 and 13. Article 10 offers a safeguard for private life, including the protection of personal data. Article 11 deals with the integrity of the human body. Article 12 presents safeguards for the home, being the physical place that may not be trespassed by outsiders without permission of the landlord. Article 13 protects the secrecy of communications. Not going into depth regarding constitutional privacy protection, it suffices to point out that privacy spans many aspects of a person's life and is not only concerned with personal data. However, due to vast and rapid datafication of many if not all aspects of daily life, the role of personal data protection as a way to safeguard privacy is growing in importance.

[4] The Cambridge Analytica case is an illustrative example. Having published original work that demonstrates the potential impact of analysing "Likes" at Facebook, Cambridge Analytica became an enemy of its own business approach when using its knowledge to nudge voters in the USA during the last presidential elections in a specific direction [15]. Cadwalladr also investigated Cambridge Analytica [16].

[5] The argument that "privacy is dead" is recurring throughout the last decades, often followed by the introduction of a novel ICT paradigm. In that sense, public perception of privacy follows a wave-pattern, not dissimilar (and perhaps the inverse of) the Gartner innovation hype cycle.

2.1 From privacy to data protection

Turning the perspective to the protection of persons with regard of the processing of their data, the OECD privacy principles play a crucial role in setting the stage. The OECD guidelines, which include the privacy principles, were formulated in 1980, and the most recent revision dates from 2013 [20]. The privacy principles are still very relevant. They cover principles concerning the limitation of the collection of data, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. The Council of Europe Convention 108 saw the light in 1981, and was the first European institutional framework that set out guidelines for dealing with personal data. The Convention has been revised in 2018, so as to align with the GDPR that is enforced from 25 May 2018 onwards [21]. The original Convention has been ratified by 55 countries [22]. The Convention was the first legally binding instrument in the field of data processing. Interestingly, the principles of the GDPR are still very much alike the principles that are present in the original Convention; both refer to the rights of data subjects and the obligations of controllers and processors, the tasks and responsibilities of supervisory authorities and the rules to abide in case of transborder data flows.

An obvious distinction that can be made between the legal instruments dealing with privacy and legal instruments dealing with data protection is the focus of the instruments. With privacy, the focus is on the substantive core of what is at stake. Privacy concerns an infringement of personal or relational space either in physical or in virtual terms. This infringement results in a form of damage, which can be physical, financial, reputational or psychological such as fear of being targeted, of being suspected, of not feeling safe in one's own surroundings anymore. With data protection, the focus is on procedures followed and taken into account, such as having performed a risk assessment, or having informed data subjects over the data that is collected. Contrary to the previous Data Protection Directive (and its implementations in national laws), the GDPR is not solely focused on procedural elements but has some substantive aspects as well. This is for instance eminent in the risk approach that is part of the GDPR. Though one might stipulate the risk assessment as described in the GDPR is a procedural one – requesting the need to identify risks and to take necessary precautionary measures – part of the GDPR is the explanation of what should be considered high risks and thus in need of a full-fledged data protection impact assessment. This clearly is more than just a procedural obligation. The same goes for a novel aspect within the GDPR concerning data protection by design and by default. Again, one might argue that the GPDR itself does not offer much support to understanding how data protection by design (or by default) should be interpreted. Along the present indications in the GDPR concerning data minimisation and pseudonymisation, the European Data Protection Board (EDPB) has released a draft version of its guidelines on data protection by design and by default.[6]

[6] The stipulations of the EDPB concerning data protection by design and by default (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en; last accessed: 29/11/2019) are in line with international developments taking place in standardisation organisations such as ISO. Work on privacy

The GDPR is large, far-reaching and includes substantive and procedural elements, which may give rise to innovative practices. A drawback is however the present uncertainty on how to understand specific elements from the GDPR. The uncertainty about how for instance data protection by default should be interpreted limits interest in developing products or services that may help in implementing data protection by default.

2.2 Companies active in data protection

For sure, the GDPR has given an impetus to companies offering products and services to organisations that need to comply with the GDPR. The offers relate to practical issues such as keeping a registry of data processing activities, keeping track of reception of requests of data subjects, organising procedures in case of identified data breaches, etc. Some companies offer more advanced tooling that enables organisations to track the maturity of their approach, to install data governance procedures, to have advanced access management and logging protocols, etc.

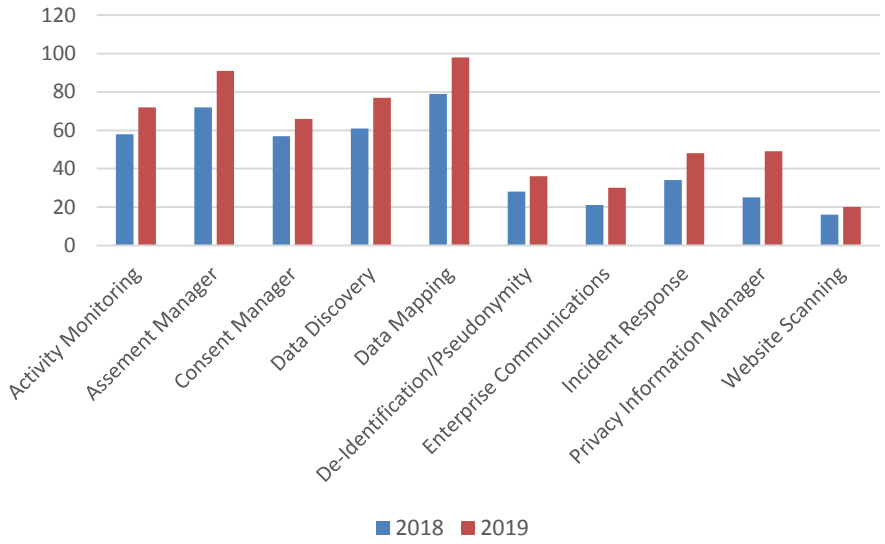

Fig. 1. Number of vendors active per product category 2018–2019 [23, 24].

management issues is performed by ISO/IEC JTC 1/SC 27/WG 5. Other organisations, such as the International Privacy Engineering Network, which has been established by the European Data Protection Supervisor, are also working on templates and guidelines to help organisations in practical tooling for integrating data protection by design and by default (https://edps.europa.eu/data-protection/our-work/subjects/ipen_en; last accessed: 23/10/2019). They all contribute to the substantive kernel of what should be considered legitimate implementations of data protection by design and by default.

The International Association of Privacy Professionals (IAPP) produces annual reports (starting in 2018) in which it presents an overview of vendors active on the market of data protection products and services. The reports are based on self-selection, i.e. vendors were offered the opportunity to provide information about their activities in the report.

The overall growth of companies offering data protection products and services was around 20% between 2018 and 2019. Figures presented in older reports show that the rise was rather linear over the past few years [24]. Fig. 1 illustrates the absolute increase in vendors per category over the last few months. Although the figures in these reports should be interpreted with caution (given that they are based on self-selection), they clearly indicate a flourishing and maturing market for data protection products and services. We will turn to these arguments in the following section.

3 Two takes on privacy markets

When it comes to innovation, it is relevant to keep the focus on the interrelationship between privacy, data protection, and measures and tools that promote or hinder the development of new data-driven products and services. With advanced technologies like AI taking off, the need for data is greater than ever and much of it comes from consumers.

The GDPR and other modern laws dealing with privacy and data protection such as the California Consumer Privacy Act become an operational reality and catch the attention of corporate leadership. Countries and jurisdictions around the world are increasingly adopting their own privacy-focused regulations. China and Russia are already installing local data residency requirements for citizens. At the same time, awareness for privacy is growing on the individual and the organisational level. This is not only the result of laws in general and new data breach notification obligations in particular but also of growing public interest in and increased sensitivity for the topic. People are beginning to understand that their data is vulnerable to disclosure without their consent. They demand organisations to take the accountability for securing their data and to comply with the laws. Privacy and security breaches pose an augmenting threat not only to users but also to system operators and designers.

The recent developments affect the market in two fundamental ways. First, the number of companies that offer privacy tools is on the rise. This is an emerging subsector of the industry that is related to the data storage sector and the security sector. Second, companies in all sectors, especially those where personal data plays a key role, not only comply with the law but go beyond it to distinguish themselves positively from their competitors.

3.1 Tools focusing on privacy protection

The rising demand for accountability forces organisations to adopt privacy technology. As stated in the previous section, the privacy technology vendor market continues to mature as more and more organisations adopt tools that help automate and streamline

privacy functions [24]. More specifically, the global market for privacy technology (the study uses the term "privacy management software") is accounted to 521.3 million US dollars (107.9 million in Europe) in 2018 and is expected to grow at a compound annual growth rate (CAGR) of 13.7% during the forecast period 2019-2027, to account to 1,585.8 million US dollars by 2027 [25]. Another study even expects a CAGR of 33.1% for the period 2019-2025. This study accounts the 2018 global market to 450 million US dollars [26]. By 2025, the study authors expect the market to account to 3,289 million US dollars.

Although the expected growth rates differ considerably, the studies agree that the global market will grow strongly in the coming years. Europe is anticipated to be the fastest growing market and North America to be the highest revenue contributor. Companies are emerging to capitalise on the growing demand for data privacy tools, both for regulatory compliance and consumer peace of mind [27]. Several such companies including, for instance, OneTrust, TrustArc, Privitar and BigID have raised sizable sums of cash for various privacy, data protection and compliance offers.[7]

The market is fragmented with the presence of several industry sectors and the lack of international coordination regarding regulations. Competition is expected to intensify in the coming years. One factor that will affect the dynamics is how international companies – that go beyond paying lip service to the laws – approach privacy. Generally, they pursue one of two approaches. They apply the tightest standards on a global basis or assess the risks and act by region. Apple stated that it is modifying its products to comply with the GDPR, and the modification will be worldwide for everyone; Facebook, in contrast, stated that they might implement extra protections for Europeans to comply with the GDPR, which will not be rolled out to people in other jurisdictions [29]. In the medium run, it is possible that the EU will become an exporter of norms that have the potential to lead to technological changes globally. However, it is also possible that certain cutting-edge technologies may not access, or have delayed access to the EU market due to regulations [30].

3.2 Privacy-friendly products and services

In a survey conducted in 2018, 75% of adults stated that they will not buy a product from a company – no matter how good its products are – if they do not trust the company to protect their data [31]. Companies compete for information and derive revenues both from purchases as well as, in a secondary market, from disclosing consumer information. Casadesus-Masanell and Hervas-Drane expect consumer awareness of disclosure practices and familiarity with the implications of the disclosure of personal data to increase [32]. They found competition to drive the provision of services with a low level of consumer information disclosure (i.e., a high level of privacy).

Protecting privacy met with considerable public interest with the refusal of Apple to grant US law enforcement backdoor access to the iPhone of a known terrorist. Indeed,

[7] End of October 2019, another announcement was made by Very Good Security, a US-based company, that was able to raise 35 million US dollars for developing tools and services that help protecting consumer privacy [28].

headlines about the matter directly addressed the notion of using privacy as a strategy by referring to the government prosecutors' quote that Apple's refusal "appears to be based on its concern for its business model and public brand marketing strategy" [33]. Beyond Apple, which seems to be willing to sacrifice some profit for the sake of privacy to bolster its image as a company that protects consumers [34], companies increasingly compete on the basis of strong privacy protections. The term "privacy as a strategy" is used to refer to the phenomenon of using data protection approaches for competitive differentiation [35].

Using privacy as a strategy remains viable as long as companies compete in markets where measures for privacy protection can be differentiated and are valued by consumers. Higher competition intensity in the marketplace does not necessarily improve privacy when consumers exhibit low willingness to pay. Therefore, privacy-friendly products and services remain niche offers. Products and services such as search engines, e-mail clients, web browsers or messenger services (e.g., DuckDuckGo, ProtonMail, Tor, Signal) that protect the privacy of users usually do not strive for economic success, but are willing to sacrifice business profits in turn of remaining close to privacy idealism.

4 Challenges and ways forward

Privacy and ICT innovation are interrelated. While the market for privacy protection tools is expected to continue to grow steadily over the next decade, the market for privacy-friendly products and services remains a niche market for the time being. Although awareness for privacy is growing, most decision makers are not willing to invest more than necessary into making products and services more privacy friendly or to use privacy-friendly products and services. Privacy and data protection have the potential to enable innovation but several challenges need to be addressed in order to make privacy markets a success across the spectrum. Key challenges are lack of profitability of privacy-friendly offerings, conflicts with new and existing business models, low value attached to privacy by individuals, latent cultural specificities, skill gaps and regulatory loopholes. These challenges, which make matching privacy harms with adequate technical tools extremely difficult, hamper the scaling and adoption of standard privacy-preserving technologies, and are reinforced by the multitude of sectoral and regulatory requirements, are outlined in the following paragraphs.

Making products and services privacy friendly leads to additional costs for both developers and users. Acquisti et al. clearly state that there are costs associated with the act of protecting privacy [36]. These costs must be offset by the expected benefits. Only then will a higher level of privacy protection make sense from an economic point of view. Examples for costs that may be incurred include costs for hardware and software as well as costs caused by user inconvenience [37]. In addition to regulatory compliance, the benefits may include reduced employee need to deal with privacy breaches (e.g., for dispute resolution) and improved reputation. There is no evidence that privacy-friendly products and services will lead to increased sales for developers or justify significantly higher prices.

Data-driven innovation may involve methods and usage patterns that neither the entity collecting the data nor the data subject considered or even imagined at the time of data collection. Putting privacy principles such as purpose limitation or data minimisation into practice may thus be in conflict with current or desired business models [38]. Moreover, conflicts may arise from different treatments of special categories of data and legal rules governing decision-making processes. Closely related to business model conflicts is the trade-off between privacy protection and the utility of data. It was found that increased data protection limits flexibility and innovation in contexts such as health care or smart cities [39, 40]. One should however be cautious in taking this argument strictly at face value. In the Netherlands, health data scientists objected to the strict rules they had to follow, complaining that this would curtail innovation. However, this approach met with opposition, accusing the data scientists of behaving irresponsibly and having insufficient eye for the potential to use the data within the limitations of the regulatory framework.[8] Moreover, carelessness, or recklessness in dealing with personal data increasingly adds to reputational damage and lack of trust, indirectly also leading to a slowing down of innovation, especially if seemingly obscure personal data processing practises are being exposed [[41]].

Individuals have the potential to exert significant pressure on actors in the data value chain. However, it was found that where there is a privacy difference between companies, the slightly cheaper but less privacy-friendly company typically obtains a greater market share [42]. Moreover, individuals do not always act in a fully rational way in situations where their privacy is affected. Therefore, privacy valuations cannot be precisely estimated [43]. Privacy concerns and expectations are remarkably context-dependent and very difficult to predict. For instance, people perceive losses differently than gains and are more willing to prevent a loss than achieve a similar gain, are risk averse, tend to overvalue immediate rewards and undervalue long-term rewards, tend to mimic behaviour shown by predecessors and behave differently in the absence of real choices [44].

Acknowledging that privacy preferences and practices vary among nations and regions is important. A universal regulatory approach to privacy would ignore cultural and societal differences. Millberg et al. state clearly that "one size does not fit all" with respect to regulatory implementation [45]. Cultural values can influence people's privacy perceptions such that countries with tighter privacy regulations tend to experience fewer privacy problems [46]. Bellman et al. found that cultural values have an impact on the extent to which errors in databases and unauthorised secondary use raise privacy concerns [47]. Opinions differ as to whether data-driven innovation leads rather to de-individualisation and discrimination, or to personalisation. Van Wel and Royakkers, for instance, state that anonymous profiling could be harmful, and lead to possible discrimination and de-individualisation [48].

---

[8] Financieel Dagblad, "Medisch onderzoek in het gedrang door strenge privacyregels", 23/09/2019. In response, the Minister of Health released a letter indicating the opportunities that researchers may refer to in having health data processed for research purposes. Minister VWS. "Reactie Artikel FD over secundair gebruik data." 1587082-195476-DICIO. 04/10/2019.

Adapting to a new mindset seems to be necessary as data has become a strategic business asset and privacy a threatened value. Failures in data security and governance regularly create public embarrassments for companies [49]. Today, according to Miller, those in charge of data must have skills ranging from math and statistics, machine learning, decision management and computer science to data ethics, law and information security [50]. Several of these skills are essential for developers to make sure privacy-preserving features are properly integrated into products and services as well as daily business practices. According to Kshetri, data-driven products and services are likely to affect the welfare of unsophisticated, vulnerable and technologically inexperienced users more negatively than others [51]. Digital literacy is a key skill in the age of big data [52].

The flexible interpretation of privacy and data protection is both a blessing and a curse for practitioners. Specific rules for the protection of special categories of data (i.e., sensitive data), which are included in the GDPR and other regulations, are embraced to a different extent by professionals. Some healthcare professionals, for instance, have seen strict privacy protection as an impediment for epidemiological research [53]. Regulations are also considered to have gaps and loopholes with respect to inferred data. The vast amount of data sources and their linkability points towards a direction when everybody would be identifiable through various data relations and as Purtova states data protection law would apply to everything [54].

Within the scope of the concluding session of the 14th IFIP Summer School on Privacy and Identity Management, an expert panel discussed ways forward towards privacy-friendly big data. Much attention was paid to the relationship between privacy and innovation. There was consensus among the experts that an increase in the funding available for related research and innovation is essential. While significant progress was made over the last couple of years with respect to privacy-preserving technologies, societal and economic aspects as well as the interplay of technologies and regulations on the one side and people and organisations on the other side is not yet sufficiently understood. Intensified research and innovation activities, however, are not enough. The experts also agreed that measures must be taken to support the transfer of results from the laboratories into practice. Relevant measures, mentioned by the experts, include involving a wide variety of stakeholders in research and innovation activities and promoting standardisation. It was considered as important that success stories and good practices are shared. However, it must be made sure that the specifics of different application contexts are adequately taken into account.

5 Conclusions

Flourishing start-ups offering tools for privacy protection and an increasing availability of products and services that are inherently privacy friendly show that privacy and data protection have the potential to be enablers of innovation. However, to make privacy markets a success across the spectrum, not only challenges related to profitability and business models need to be overcome, but also challenges related to the individual valuation of privacy, cultural differences, skills and regulations. Consumer trust is central

for realising businesses with data-driven products and services. Therefore, being able to demonstrate accountability in processing personal data as well as security and transparency in data archiving and storage are essential for businesses. A proactive privacy approach, which means that the legal framework is not played down but taken seriously, makes this much easier.

We are convinced that responsible use of data and being innovative fit together well; it is not necessary to choose one or the other. In the short term, taking not only laws fully into account but also additional measures to protect privacy may be more of an effort, but it will pay off in the medium and long term. Increased research and innovation and the exchange of good practices will encourage a change of mindset. This perspective was shared by the panel of experts at the IFIP Summer School. Concerning privacy as an innovation opportunity, Hasselbalch and Tranberg compared data ethics with being eco-friendly [55], "Being eco-friendly has become an investor demand, a legal requirement, a thriving market and a clear competitive advantage. Data ethics will develop similarly – just much faster."

Acknowledgements. The research leading to the presented results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreements No. 731873 and No. 732630.

References

1. Hemerly, J.: Public policy considerations for data-driven innovation. Computer 46 (6), 25–31 (2013).
2. London Economics: Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs), https://londoneconomics.co.uk/wp-content/uploads/2011/09/17-Study-on-the-economic-benefits-of-privacy-enhancing-technologies-PETs.pdf (2010).
3. Zarsky, T.Z.: The privacy-innovation conundrum. Lewis & Clark Law Review 19 (1), 115–168 (2015).
4. CISCO: Maximizing the Value of your Data Privacy Investments. Data Privacy Benchmark Study, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf (2019).
5. Dhanda, R.: Data Privacy Regulations' Implications on AI, https://securityboulevard.com/2019/09/the-implications-of-data-privacy-regulations-on-ai/, last accessed 29/11/2019.
6. Ponemon Institute: Cost of a Data Breach Report 2019, https://www.ibm.com/downloads/cas/ZBZLY7KL (2019).
7. The Harris Poll: IBM Survey Reveals Consumers Want Businesses to Do More to Actively Protect Their Data, https://theharrispoll.com/ibm-survey-reveals-consumers-want-businesses-to-do-more-to-actively-protect-their-data/, last accessed 31/10/2019.
8. Fleck, M.: How GDPR is Unintentionally Driving the Next Decade of Technology, https://www.securityweek.com/how-gdpr-unintentionally-driving-next-decade-technology, last accessed 27/10/2019.

9. Kelly, H.: California passes strictest online privacy law in the country, https://money.cnn.com/2018/06/28/technology/california-consumer-privacy-act/index.html, last accessed 31/10/2019.
10. Morsink, J.: The Universal Declaration of Human Rights. Origins, Drafting, and Intent. University of Pennsylvania Press, Philadelphia (2009).
11. Berlin, I.: Two Concepts of Liberty. In: Berlin, I. (ed.) Four Essays on Liberty, pp. 118–172. Oxford University Press, Oxford (1969).
12. Westin, A.F.: Privacy and Freedom. Simon & Schuster, New York (1967).
13. Bennett, C.J., Raab, C.D.: The Governance of Privacy. Policy Instruments in Global Perspective. MIT Press, Cambridge (2006).
14. Finn, R.L., Wright, D., Friedewald, M.: Seven types of privacy. In: Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (eds.) European Data Protection. Coming of Age, pp. 3–32. Springer, New York (2013).
15. Laterza, V.: Cambridge Analytica, independent research and the national interest. Anthropology Today 34 (3), 1–2 (2018).
16. Cadwalladr, C.: The Cambridge Analytica files. 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower, https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump, last accessed 31/10/2019.
17. Nagenborg, M.H.: Hidden in plain sight. In: Timan, T., Newell, B.C., Koops, B.-J. (eds.) Privacy in Public Space. Conceptual and Regulatory Challenges, pp. 47–63. Edward Elgar, Northampton (2017).
18. Scherr, A.E.: Privacy in public spaces. The problem of out-of-body DNA. In: Timan, T., Newell, B.C., Koops, B.-J. (eds.) Privacy in Public Space. Conceptual and Regulatory Challenges, pp. 211–241. Edward Elgar, Northampton (2017).
19. Koops, B.-J., Newell, B.C., Timan, T., Škorvánek, I., Chokrevski, T., Galič, M.: A typology of privacy. University of Pennsylvania Journal of International Law 38 (4), 483–575 (2017).
20. OECD: The OECD Privacy Framework, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (2013).
21. Council of Europe: Convention 108 +. Convention for the Protection of Individuals with regard to the Processing of Personal Data, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (2018).
22. Council of Europe: Chart of signatures and ratifications of Treaty 108, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=jHKJqtBd, last accessed 30/11/2019.
23. IAPP: 2018 Privacy Tech Vendor Report, https://iapp.org/media/pdf/resource_center/2018-Privacy-Tech-Vendor-Report.pdf (2018).
24. IAPP: 2019 Privacy Tech Vendor Report, https://iapp.org/media/pdf/resource_center/2019TechVendorReport.pdf (2019).
25. The Insight Partners: Privacy Management Software Market to 2027, https://www.theinsightpartners.com/reports/privacy-management-software-market/?HK+MD, last accessed 30/11/2019.
26. Market Study Report: Global Privacy Management Software Market Size, Status and Forecast 2019-2025, https://www.marketstudyreport.com/reports/global-privacy-management-software-market-size-status-and-forecast-2019-2025, last accessed 09/12/2019.

27. Sawers, P.: 5 data privacy startups cashing in on GDPR, https://venturebeat.com/2019/07/23/5-data-privacy-startups-cashing-in-on-gdpr/, last accessed 27/10/2019.
28. Sawers, P.: Very Good Security raises $35 million to protect companies' private customer data, https://venturebeat.com/2019/10/24/very-good-security-raises-35-million-to-protect-companies-private-customer-data/, last accessed 31/10/2019.
29. Hern, A.: What is GDPR and how will it affect you?, https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you, last accessed 27/10/2019.
30. Bachlechner, D., La Fors, K., Sears, A.M.: The role of privacy-preserving technologies in the age of big data. In: Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy (WISP 2018). AIS, Atlanta (2018).
31. IBM News Room: New Survey Finds Deep Consumer Anxiety over Data Privacy and Security, https://newsroom.ibm.com/2018-04-15-New-Survey-Finds-Deep-Consumer-Anxiety-over-Data-Privacy-and-Security, last accessed 30/11/2019.
32. Casadesus-Masanell, R., Hervas-Drane, A.: Competing with privacy. Management Science 61 (1), 229–246 (2015).
33. Lichtblau, E. and Apuzzo, M.: Justice Department Calls Apple's Refusal to Unlock iPhone a 'Marketing Strategy', https://www.nytimes.com/2016/02/20/business/justice-department-calls-apples-refusal-to-unlock-iphone-a-marketing-strategy.html, last accessed 27/10/2019.
34. Love, J.: Apple 'privacy czars' grapple with internal conflicts over user data, https://www.reuters.com/article/us-apple-encryption-privacy-insight-idUSKCN0WN0BO, last accessed 27/10/2019.
35. Martin, K.D., Murphy, P.E.: The role of data privacy in marketing. Journal of the Academy of Marketing Science 45 (2), 135–155 (2017).
36. Acquisti, A., Taylor, C., Wagman, L.: The economics of privacy. Journal of Economic Literature 54 (2), 442–492 (2016).
37. Khokhar, R.H., Chen, R., Fung, B.C.M., Lui, S.M.: Quantifying the costs and benefits of privacy-preserving health data publishing. Journal of Biomedical Informatics 50 , 107–121 (2014).
38. Zarsky, T.Z.: Incompatible: The GDPR in the age of big data. Seton Hall Law Review 47 (4), 995–1020 (2017).
39. Iyengar, A., Kundu, A., Pallis, G.: Healthcare informatics and privacy. IEEE Internet Computing 22 (2), 29–31 (2018).
40. Mazhelis, O., Hamalainen, A., Asp, T., Tyrvainen, P.: Towards enabling privacy preserving smart city apps. In: Proceedings of the 2016 IEEE International Smart Cities Conference (ISC2), pp. 1–7. IEEE, Piscataway (2016).
41. Pilkington, E.: Google's secret cache of medical data includes names and full details of millions – whistleblower, https://www.theguardian.com/technology/2019/nov/12/google-medical-data-project-nightingale-secret-transfer-us-health-information, last accessed 29/11/2019.
42. Jentzsch, N., Preibusch, S. and Harasser, A.: Study on Monetising Privacy. An Economic Model for Pricing Personal Information, https://www.enisa.europa.eu/publications/monetising-privacy/at_download/fullReport (2012).
43. Acquisti, A., John, L.K., Loewenstein, G.: What is privacy worth? The Journal of Legal Studies 42 (2), 249–274 (2013).

44. van Lieshout, M.: The value of personal data. In: Privacy and Identity Management for the Future Internet in the Age of Globalisation, pp. 26–38. Springer, London (2015).
45. Milberg, S.J., Smith, H.J., Burke, S.J.: Information privacy. Corporate management and national regulation. Organization Science 11 (1), 35–57 (2000).
46. Dolnicar, S., Jordaan, Y.: A market-oriented approach to responsibly managing information privacy concerns in direct marketing. Journal of Advertising 36 (2), 123–149 (2007).
47. Bellman, S., Johnson, E.J., Kobrin, S.J., Lohse, G.L.: International differences in information privacy concerns. A global survey of consumers. The Information Society 20 (5), 313–324 (2004).
48. van Wel, L., Royakkers, L.: Ethical issues in web data mining. Ethics and Information Technology 6 (2), 129–140 (2004).
49. Duhigg, C.: How Companies Learn Your Secrets, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html, last accessed 27/10/2019.
50. Miller, S.: Collaborative approaches needed to close the big data skills gap. JOD 3 (1), 26 (2014).
51. Kshetri, N.: Big data's impact on privacy, security and consumer welfare. Telecommunications Policy 38 (11), 1134–1145 (2014).
52. Segura Anaya, L.H., Alsadoon, A., Costadopoulos, N., Prasad, P.W.C.: Ethical implications of user perceptions of wearable devices. Science and Engineering Ethics 24 (1), 1–28 (2018).
53. Nyrén, O., Stenbeck, M., Grönberg, H.: The European Parliament proposal for the new EU General Data Protection Regulation may severely restrict European epidemiological research. European Journal of Epidemiology 29 (4), 227–230 (2014).
54. Purtova, N.: The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology 10 (1), 40–81 (2018).
55. Hasselbalch, G., Tranberg, P.: Data Ethics. The New Competitive Advantage. PubliShare, Valby (2016).