Processing purposes

TRIX MULDER

INTRODUCTION

The healthcare sector has traditionally processed large amounts of personal data. The rise of information technologies, such as smartphone applications ("apps") and wearable devices (e.g. Fitbit, smart soles) both inside and outside medical practice, has added to the processing of these kinds of personal data. Commercial apps and wearables that aim to encourage health behaviour change are flourishing in the major app stores. These technologies enable people to monitor their own health by using (pressure) sensing technologies that measure vital signs (for example, heartrate) and track progress (such as counting steps), without having to visit a doctor.[1] A new complicating factor is that these so-called commercial health apps and wearables are increasingly being used within a medical context. The data generated transcends the closed context of personal medical records, geographic borders and, in particular, the borders of the European Union. This is problematic, because no current regulations address the global dimension of data.[2]

Legislative bodies worldwide have tried to deal with this global dimension of data, and if 2018 proved one thing, it is that legal data protection is very much alive and kicking.[3] Both the European Union and the Council of Europe, the two major European legislators, updated their legal instruments relating to data protection, which originated from the last century. The Council of Europe updated their Convention 108[4] and the General Data Protection Regulation (GDPR)[5] entered into force on 25 May 2018. Outside the European Union, the State of California followed this trend with the California Consumer Privacy Act 2018 (CCPA)[6] on 29 June 2018. The CCPA will enter into force on 1 January 2020. These legal changes are required, since information technologies are evolving quickly and regulation is trying to keep up to avoid a growing gap.[7]

[1] Brad Millington, 'Smartphone Apps and the Mobile Privatization of Health and Fitness' (2014) 31:5 Critical Studies in Media Communication 479.

[2] Denis Kelleher, EU Data Protection Law (Bloomsbury Publishing Plc 2018) 109.

[3] Graham Greenleaf, ''Modernised' Data Protection Convention 108 and the GDPR' (2018) 154 Privacy Laws & Business International Report 22 < http://www.ssrn.com/link/UNSW-LEG.html > accessed 10 May 2019.

[4] Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS No. 108 (CM/Inf (2018) 15-final).

[5] European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[6] California Consumer Privacy Act (CCPA) AB 375.

[7] Andrew Askland, 'Introduction: Why Law and Ethics Need to Keep Pace with Emerging Technologies' in Gary Marchant, Braden Allenby and Joseph Herkert (eds), The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight (Springer 2011) xiii.

DOI: 10.5281/zenodo.3296915

LEGAL CHALLENGES

The use of these commercial health apps within medical practice creates several legal challenges, such as reconciling these apps with data protection laws and principles. This is especially relevant because the two major legal frameworks that regulate data protection in Europe characterise these kinds of personal data as a special category of data, also referred to as sensitive data.[8] These data protection regulations also determine that personal data can only be processed for specific, explicit and legitimate purposes.[9] This is referred to as purpose limitation. The Draft Code of Conduct on privacy for mobile health applications also acknowledges this principle.[10] This research offers an analysis of the principle of purpose limitation in European data protection law and examines how the privacy policies of health apps deal with this principle in practice so that legal obstacles to using commercial health apps in a medical practice can be revealed. Furthermore, it will discuss lawful ways to handle such obstacles. This could increase adoption of commercial apps in clinical practice and affect the development of the next generation of health apps.

MODERN TECHNOLOGIES

Well over 320,000 health apps[11] are available on the major app stores (Apple, Google and Microsoft). For example, Fitbit has over 25 million active users worldwide, the Nike app registers over 1.8 million workouts per month worldwide and 8 million activities are uploaded on the Strava app every day, worldwide. This shows that health apps are an important part of our global society. However, global regulation on data protection is lacking.[12] Furthermore, it is not always clear how the companies that offer these eHealth technologies and services protect the health data they generate. It is thus not surprising that the digital transformation of health and care has become a priority EU issue. See for example, the communication on enabling the digital transformation of health and care in the digital single market, empowering citizens and building a healthier society.[13]

Because of the large number of different health apps in the three major app stores (Apple, Google and Windows/Microsoft), investigating all these apps would go beyond the scope of this exploratory research. This research offers purely theoretical observa-

[8] Article 9 GDPR and Article 6 Modernised Convention 108.

[9] Article 5 (1,c) GDPR and Article 5 (4,b) Modernised Convention 108.

[10] Draft Code of Conduct on privacy for mobile health applications < https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised > accessed 13 May 2019, 7.

[11] Sometimes literature uses the term "lifestyle apps" or "wellbeing apps" to describe apps that aim health behaviour change. In this paper, I chose to use the term "health apps" to refer to these apps.

[12] Kelleher (n 1) 109.

[13] Brussels COM 2018, 233 final.

tions on the question whether the purposes used in the analysed privacy policies match the purposes used by the healthcare sector.[14] Three local rehabilitation centres in the Netherlands showed interest in this research and offered their cooperation.[15] Via a short questionnaire, physicians in these three rehabilitation centres were asked three questions about apps they already use, apps they want to use and apps patients suggested using.[16] In total, 34 different apps were mentioned by at least one physician. These apps were selected for this research. At the end of the research period, four apps were no longer available, which left this research with thirty apps.

PURPOSE LIMITATION IN EUROPEAN PRIVACY LAWS

The GDPR and modernised Convention 108 determine that purpose limitation is one of the general principles relating to the processing of personal data. It means that personal data can only be collected for specified, explicit and legitimate purposes and cannot be processed further in a manner that is incompatible with the original purposes for processing.[17] Since purpose limitation is a general principle, it applies both to the processing of sensitive data and other (non-sensitive) personal data. Both the Council of Europe and the European Union have deemed purpose limitation a "key principle and stable element" regarding data protection legislation for years.[18]

Due to the principle of purpose limitation, personal data cannot be processed for other purposes than the purpose for which the personal data was originally intended. If someone wants to process the personal data for another purpose, the data subject's consent is needed in most cases.[19] In the case of sensitive data, regular consent is not enough. Either explicit consent is needed[20] or appropriate safeguards have to be enshrined in law.[21]

The GDPR offers guidelines for controllers by pointing out five elements controllers have to take into account to help determine whether processing for another purpose is

[14] Robert Yin, Case Study Research, Design and Methods (5th edn, Sage Publications 2014) 40.

[15] Beatrixoord, Roessingh and De Hoogstraat.

[16] The questions were: 1. Do patients ever suggest using an app or wearable in their rehabilitation process that they already use or would like to use and, if so, which apps and wearables are this and where do they want to use them for? 2. Have you ever advised an app or wearable yourself and, if so, what apps or wearable and for what part of the rehabilitation process?; 3. Are there apps or wearables that you have not yet advised, but would like to advise and if so what would that app or wearable be suitable for?;
One of the revalidation centers conducted a similar inquiry themselves a few weeks earlier, therefore the data of those questionnaires where used instead of the questions above.

[17] Ibid (n 9).

[18] Nikolaus Forgó, Stefanie Hänold and Benjamin Schütze, 'The Principle of Purpose Limitation and Big Data' in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (eds), New Technology, Big Data and the Law (Springer 2017) 22.

[19] Article 6 (1,a) GDPR and Article 5 (2) Modernised Convention 108.

[20] Article 9 (2,a) GDRP.

[21] Article 6 (1) Modernised Convention 108.

compatible with the original purpose.[22] Although the list is not exhaustive, it does give the controller some guidance. First, the controller has to take into account "any link between the purposes for which the personal data have been collected and the purposes of the intended further processing".[23] Second, the "context in which the personal data have been collected, in particular regarding the relationship between data subject and the controller"[24] are important. Third, the "nature of the personal data, in particular whether special categories of personal data are processed"[25] has to be taken into account. Also, the "possible consequences of the intended further processing" for the data subject have to be considered. Finally, the "existence of appropriate safeguards",[26] including encryption or pseudonumisation, have to be taken into account.

Before any conclusions can be drawn on the question of whether or not the purposes for processing the personal data collected via commercial apps and wearables are compatible with the processing of that personal data in a medical context, the processing purposes of both have to be mapped out so they can be compared.

PURPOSES FOR PROCESSING PERSONAL DATA

This paragraph will describe the processing purposes of commercial health apps and wearables and those of the healthcare sector.

Healthcare sector

In the healthcare sector, there are several purposes for processing personal data from patients. The most important ones are to provide patient care and to support the administration of patient care. Processing is also necessary for billing and for submitting reimbursement claims to healthcare insurance companies.[27] In university medical centres, personal data might also be processed for research purposes.

In most cases, personal data collected via commercial health apps and wearables will be used in a patient treatment plan. Therefore, the purpose of processing these kinds of data will correlate with the first purpose: providing patient care. Data concerning health cannot be processed unless one of the exemptions mentioned in Article 9 (2) are met. For medical treatment, Article 9 (2,h in conjunction with 3) GDPR allows the processing of these kinds of data when these data are necessary for a medical diagnosis and they are being processed by or under the responsibility of someone who is subject to the

[22] Article 6 (4) GDPR.

[23] Ibid.

[24] Ibid.

[25] Ibid.

[26] Ibid

[27] For example: Processing of Patient Personal Data, a guideline for General Practitioners 2018.

obligation of professional secrecy. Although it could be argued that data collected via commercial health apps and wearables are necessary for a medical diagnosis, the data are not being processed by or under the responsibility of someone who is obliged to maintain professional secrecy. Therefore, the explicit consent of the data subject is needed.[28] Even though this could be arranged, there is another problem regarding the processing of these kinds of data in a medical context. This has to do with the way the processing purposes are described in the privacy policies of these commercial health apps and wearables.

Privacy policies and purposes

Commercial apps and wearables usually ask the user for consent to the processing of their personal data via privacy policies. Our investigation of several privacy policies of commercial health apps and wearables showed that the purposes for processing are typically quite vague. For this research, we analysed thirty privacy policies. The privacy policies do not use a standard format; therefore, we identified 19 different processing purposes, ranging from providing services to marketing and sharing with third parties. A complete overview of the purposes, with an example, can be found in Table 1.

As Table 1 shows, most of these purposes are explained in rather vague terms. The privacy policies mention, that the companies want to use the personal data to "improve and maintain products and services", without being clear on what part of the personal data are being used for this purpose and what "products and services" are meant. Other privacy policies mention that they process personal data, such as the "use of workout data". Although the privacy policy does mention that the nature of these data are "in some jurisdictions" considered to be sensitive data, the privacy policy does not elaborate on how these data are used. It only mentions that the company will "take appropriate measures in protecting and using this data and (…) will obtain consent before they use these kinds of data."

Although this is only a small selection of the vague processing purposes, it makes clear that most of these vague descriptions are not in accordance with the GDPR. After analysing thirty privacy policies, it was still very hard to determine the exact purposes for processing personal data and therefore it was not clear what the user had to consent to. The implication of this is as follows: if we do not take action, we will lose purpose limitation as a safeguard for data protection. After all, if we do not know what we are consenting to when we agree to privacy policies, this might affect the validity of our consent.

[28] Article 9 (2,a) GDPR.

TABLE 1: PURPOSES FOR PROCESSING PERSONAL DATA

Purpose	Example
Provide service	To improve and maintain products and services
Administer service	For customer support
Users experience	To personalise and improve your experience
Provide care	To provide care
Medical procedure /treatment	The most important place we store your data is in the Electronic Patient File
Declaration of healthcare costs	To declare healthcare costs (to insurers or the patient)
Information provision	For software updates, events, products
Dealing with complaints	We process your personal information when you contact us to help you with any questions, concerns, disputes or issues
Communication with user	To send the user service notifications and respond to the user
Qualitative goals	To enhance and improve application
Safety and security	For the safety and security of the services, users and other parties
Legal obligations	To fulfil legal obligations or to protect from legal claims
Research	To understand customer behaviour or preference
Marketing purposes	Advertise and market to users, which includes sending promotional communications, targeting advertising, and presenting you with relevant offers
Sales activities	Processing orders
Identity confirmation	We may use your personal data to confirm your identity
Management operations	Supporting operational management
Audits	We may also use your personal data for internal matters, such as audits and data analyses
Sharing with third parties	To help advertisers and other partners measure the effectiveness and distribution of their ads and services and their users

CONCLUSIONS

Although the privacy regulations implemented in Europe in 2018 determine that purpose limitation is a key concept in data protection, the privacy policies of commercial health apps do not comply with these rules. This is despite the fact that the Draft Code of Conduct on privacy for mHealth apps acknowledges purpose limitation as a key element in data protection, especially regarding data concerning health. Therefore, the use of these commercial apps and wearables in a medical context is difficult. This is particularly relevant because data protection laws in Europe categorise health data as sensitive data, which can, in principle, not be processed. Further cooperation between the European Data Protection Board (EDPB) and representatives of app providers and the healthcare sector on this matter is desirable, given that, together, they can create solutions that benefit all, including data subjects. This will make it easier for all app providers to comply with the GDPR and the modernised Convention 108, taking account of the particular needs of the healthcare sector, and it will support national supervisory authorities in enforcing these regulations.

BIBLIOGRAPHY

Askland A, 'Introduction: Why Law and Ethics Need to Keep Pace with Emerging Technologies' in Gary Marchant, Braden Allenby and Joseph Herkert (eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight* (Springer 2011).

Brussels COM 2018, 233 final.

California Consumer Privacy Act (CCPA) AB 375.

Convention for the protection of individuals with regard to automatic processing of personal data [1981] ETS No. 108 (CM/Inf (2018) 15-final).

Draft Code of Conduct on privacy for mobile health applications <https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised>

European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

Processing of Patient Personal Data, a Guideline for General Practitioners 2018.

Forgó N, Hänold S and Schütze B, 'The Principle of Purpose Limitation and Big Data' in Corrales M, Fenwick M and Forgó N (eds), *New Technology, Big Data and the Law* (Springer 2017).

Greenleaf G, ''Modernised' Data Protection Convention 108 and the GDPR' (2018) 154 Privacy Laws & Business International Report 22. http://www.ssrn.com/link/UNSW-LEG.html (accessed 10 May 2019).

Kelleher D, *EU Data Protection Law* (Bloomsbury Publishing Plc 2018).

Millington B, 'Smartphone Apps and the Mobile Privatization of Health and Fitness' (2014) 31:5 Critical Studies in Media Communication.

Yin R, *Case Study Research, Design and Methods* (5th edn, Sage Publications 2014).