UNIVERSITY OF TURKU

This is an Accepted Manuscript version of the following article published originally by Springer, accepted for publication in the proceedings:

Information Systems and Technologies : WorldCIST 2023, Volume 1

This version may differ from the original in pagination and typographic details. When using please cite the original.

AUTHOR(S)	Carlsson R., Rauti S., Mickelsson S., Mäkilä T., Heino T., Pirjatanniemi E., Leppänen V.
TITLE	Several Online Pharmacies Leak Sensitive Health Data to Third Parties.
YEAR	2024
DOI	10.1007/978-3-031-45642-8_16
CITATION	Carlsson, R. et al. (2024). Several Online Pharmacies Leak Sensitive Health Data to Third Parties. In: Rocha, A., Adeli, H., Dzemyda, G., Moreira, F., Colla, V. (eds) Information Systems and Technologies. WorldCIST 2023. Lecture Notes in Networks and Systems, vol 799. Springer, Cham. https://doi.org/10.1007/978-3-031-45642-8_16
VERSION	Accepted Manuscript
LICENSE	In Copyright © 2024 The Author(s), under exclusive license to Springer Nature Switzerland AG

Several online pharmacies leak sensitive health data to third parties

Robin Carlsson[1], Sampsa Rauti[1], Sini Mickelsson[1], Tuomas Mäkilä[1], Timi Heino[1], Elina Pirjatanniemi[2], and Ville Leppänen[1]

[1] University of Turku, 20014 Turku, Finland,
crcarl@utu.fi, sjprau@utu.fi, sini.mickelsson@utu.fi
tusuma@utu.fi, tdhein@utu.fi, ville.leppanen@utu.fi
[2] Åbo Akademi, Turku, Finland,
elina.pirjatanniemi@abo.fi

Abstract. As the demand for digital services keeps growing, online pharmacies have become a very important part of essential digital services. When sensitive personal data such as medicine orders are processed, privacy issues become increasingly important. In this paper, we take a look at personal data delivered to third parties in 20 Finnish online pharmacies. More specifically, we study whether the data on prescription medicine orders is leaked out to third-party analytics services. Our findings reveal that 14 (70%) of studied pharmacies send out information about the customers intending to order prescription medicines to third parties, and 7 (35%) of the pharmacies even leak the data about the specific prescription medicine a specific customer is ordering. We also discuss implications of the data leaks and give suggestions on how this alarming state of affairs can be alleviated.

Keywords: Online pharmacies, Web privacy, Network traffic analysis, Data concerning health

1 Introduction

Digital technologies are a powerful tool for delivering essential services when customers have challenges in using services onsite. Especially many vulnerable people such as the elderly, those with serious health conditions, and sometimes people living in rural areas can benefit from digital services [17]. As connectivity has improved and services can reach a greater portion of the population, legislators have also understood the importance of digital service delivery. In Finland, for instance, the Act on the Provision of Digital Services (306/2019) was passed in 2019 in order to improve the accessibility, quality and security of digital services and allow everyone to use them equally. The COVID-19 pandemic has only made the need for online services more pronounced and accelerated the digital transformation [2].

As the demand for digital services rises, online privacy issues also become increasingly important. One very important example of essential digital services

are online pharmacies, which we are focusing on in this paper. Sensitive information such as prescription medicine orders are processed in these services, making strict data privacy vitally important. The traditional brick-and-mortar pharmacies are obliged to keep confidential the information regarding the customer's medical conditions, unless there is a lawful basis to turn the information over to third parties such as the customer's explicit consent or a legal obligation. The pharmacies are presumed only to use the information on the customer's medication for the purpose of achieving good patient care and to comply with their mandatory obligations. It is also important to set up the pharmacy facilities so that customers can do business privately and confidentially.

In the current digital world, however, the same principles of confidentiality and privacy do not always appear to be followed so well in practice. Third-party analytics services and tracking mechanisms are widespread across the web [13, 19], even in essential web services and on websites maintained by public sector bodies [6, 18]. In several essential online services, sensitive personal data can be unintentionally delivered to third parties if the developers and data protection officers have not been careful when designing websites. With this in mind, the current study conducts a network traffic analysis for 20 Finnish online pharmacies in order to find out whether personal data and sensitive information is being leaked to third-party analytics services.

The contributions of this paper are as follows. Along with Zheutlin et al.'s study on data-tracking in online pharmacies [20], to the best of our knowledge, the current study is one of the first studies to address third-party tracking in online pharmacies. In their brief article, Zheutlin et al. discuss the prevalence of data tracking among online pharmacies but do not go into the detail about what kind of data is shared to the third-party analytics services. The current study not only researches whether tracking happens and is widespread, but also provides a technical analysis on personal data shared with third parties and investigates whether sensitive information is being delivered to analytics services in several online pharmacies. In our technical analysis, we focus on the use case in which a customer searches and places an order for a prescription medicine. Specifically, we want to find out whether the intent to order a specific prescription medicine is leaked out to third parties. In doing so, the authors also revealed serious data leaks among several Finnish online pharmacies. We have reported these privacy issues to the appropriate authorities, and one of the studied pharmacies has already made significant changes to its website and privacy practices. Finally, the current study discusses the implications of our results for web development and online pharmacies in general.

The rest of the paper is organized as follows. Section 2 reviews the related work. Section 3 introduces the setting of the study, the used data set and methodology. Section 4 discusses the results of the study, providing an analysis on personal data the studied online pharmacies leak to third parties. Section 5 discusses the implications of our key findings and provides some guidelines to improve the privacy of online pharmacies. Finally, Section 6 concludes the paper.

2 Related work

Zheutlin et al. [20] study the prevalence of data tracking among online pharmacies. Among accredited digital pharmacies in the US, analytics services were found to be common, with over two-thirds of the studied pharmacies using at least two third-party services to capture user data. The most prevalent data-tracking services were Facebook and Google Analytics. While the authors do note that the results raise concerns about how health data – such as information on prescription medication – is shared, they do not present any more details about the nature of the data delivered to the third-party analytics services. Therefore, our current study can be seen as a continuation of their work, although the set of studied pharmacies is different.

In a recent study, Huo et al. [7] studied potential health data leaks and analytics on 459 online patient portals and 4 telehealth websites. Their findings indicate that 14% of patient portals include Google Analytics. Also, 9 websites contained services disclosing sensitive health data, such as medications and laboratory results, to third parties. It is quite obvious that many health care operators and maintainers of health related websites do not always have the necessary technological skills to detect or fix these problems. Indeed, in several medical studies (see e.g. [15] and [8]), analytics services are still being used as a part of health related web platforms, most likely without fully realizing the risks involved. The results of Huo et al., just like the findings of our current study, highlight a lack of privacy by design approach, and put emphasis on the importance of educating website developers and data protection officers about this issue.

In a similar vein, Zheutlin et al. studied data-tracking on government, non-profit, and commercial health-related websites [21]. The results indicate that it is relatively common for health-related websites to provide information to third-parties, the average number of analytics services on the studied websites was 2.11. Unfortunately, in many cases, finding and displaying health information online is not a private action. This problem does not only concern health-related websites but many other critical services as well. Recent studies have shown that even many public sector bodies can leak sensitive information to third parties from their websites [6].

Finally, it is also important to have the appropriate tools and methods for studying network traffic and compliance issues on websites. The users need to know if websites really act according to their data privacy choices. Martinez et al. [10] present new algorithms and a measure to assess user tracking compliance and the confidence in the analytics services. From a technical viewpoint, it is necessary to be able to accurately identify personal data from internet traffic when researching what kind of information is delivered to analytics services. To this end, Liu et al. [9] develop a new method of discovering various types of personal data carried within network traffic.

3 Study setting and methodology

From the list of legal Finnish online pharmacies[3] maintained by the Finnish Medicines Agency, Fimea, 20 online pharmacies were chosen to be studied. If a chosen online pharmacy did not sell prescription medicines at all, the pharmacy was discarded from the set of selected pharmacies and a new one was chosen at random. In this study, we chose not to refer to the pharmacies by their real names, but instead call them Pharmacies 1–20.

The online pharmacies were tested by first navigating to the store page, clearing the browser cache and cookies and then reloading the page. From reloading onwards, all the network traffic associated with use of the pharmacy was captured using Google Chrome's DevTools. The cache was disabled while recording and the captured traffic was preserved as a HTTP Archive file. When arriving at the pharmacy website, all cookies were consented to upon request.

While the exact navigation on websites varies between the studied online pharmacies, the experiment was always continued until the intent to order a prescription medicine was clear — for example, a button for ordering a specific medicine was pressed or the medicine was successfully added as part of the order. The goal was to find out whether the intent to order a specific prescription medicine was delivered to third-party analytics services. To place a final order, chatting with a pharmacist is required in Finnish online pharmacies. We ended our experiment before this phase.

The 20 online pharmacies tested all provided a search bar, and the name of a prescription medicine was entered into the search. If the product came up in the search (i.e. prescription medicines were searchable items), its product page was opened. Finally, if the product page led to a separate page for ordering the product, that page was also accessed to see whether sensitive information about the user's intent to purchase this prescription medicine was sent to analytics services.

If the prescription medicine was found in the search and the product page was accessed, but no separate page for ordering the product was available, we registered and logged into the online pharmacy to initiate an order. After registering, the ordering process was continued until contact with a pharmacy assistant was required.

If prescription medicines were not available in the search, but the pharmacy offered a link or button for beginning the ordering process directly, this option was used instead. An order was initiated, and the correct product was then selected to be part of the order. The ordering process was interrupted before requesting that a pharmacy assistant contact the user.

Moreover, after running the experiments described above, the privacy policies of the chosen online pharmacies were analyzed. Each privacy policy document was read to find out whether anything about sending data on ordered prescription medicines to third parties was mentioned. The studied privacy policies were

[3] https://www.fimea.fi/apteekit/verkkopalvelutoiminta/lailliset_apteekin_verkkopalvelut

analyzed by two researchers and any disagreements were discussed until agreement was reached.

Finally, we briefly summarize what is meant by the term *personal data*. In this paper, the term is given the same meaning as in the EU General Data Protection Regulation (GDPR)[4]. Pursuant to Article 4(1) of the GDPR "personal data" refers to any information relating to an identified or identifiable person, in other words, data based on which an individual can be identified directly or indirectly. According to the GDPR a person can be identifiable specifically based on a reference to an identifier such as name, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the said person. In general, the scope of the term is considered to be broad and further expanding (see e.g. [3], [1]; [4, p. 113], [12, p. 41–42]).

4 Results: analysis on personal data sent to third parties

Table 1 shows the third-party analytics services that were found on the pharmacy websites while performing our experiments and recording network traffic. We can see that only 6 pharmacies did not have any analytics on the pages we tested. Pharmacies 1 and 2 had 4 different third-party services, which can be considered a large number as we only followed a path consisting of a few different pages. When there were any analytics services on the studied website, Google was almost always present, except in two cases where Pingdom, a Swedish website monitoring service was used. Other frequently appearing third-party services were Facebook and Giosg. The latter is not an analytics service per se but rather a company providing live chat services. Sensitive information about the user's identity and actions was sent to this company nevertheless.

The data sent to third parties contains items such as IP addresses, device and user specific identifiers, User-Agent headers with information on operating system and browser, and other technical pieces of information such as screen size. When it comes to identifying the user, an important piece of data is often the device's IP address, which is delivered along with every web request.

According to the preamble to the GDPR, in determining whether a person is identifiable, all the means reasonably likely to be used to identify the person directly or indirectly should be taken into consideration. This includes all objective facts, such as the costs and the amount of time required for identification as well as the available technology and technological developments.[5] Pursuant to the case Breyer of the Court of Justice of the European Union, IP addresses can

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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/EU (General Data Protection Regulation). Official Journal of the European Union, L 119, 4 May 2016.

[5] Recital 26 of the preamble to the GDPR

be considered as personal data even if identifying of a person requires acquiring additional information from a third party [1].

In accordance with recital 26 of the GDPR, data protection provisions do not apply to anonymized information. Google Analytics, for example, can be configured to anonymize data by removing the last octet of the user's IP address. It is questionable, however, whether this anonymization renders data anonymous "in such a manner that the data subject is not or no longer identifiable". This is because even if the IP address is partially anonymized, lots of other technical information is sent along it, making identification of the user possible, especially for big data collectors such as Google. Taking all this into consideration, it can be argued that in the case of the studied online pharmacies, a significant risk exists that the data could be linked to the person visiting the website.

Table 1. Pharmacies and detected third-party analytics services.

	Third-party analytics services
Pharmacy 1	Facebook, Giosg, Google, New Relic
Pharmacy 2	Crazy Egg, Facebook, Giosg, Google
Pharmacy 3	Google
Pharmacy 4	Facebook, Google
Pharmacy 5	
Pharmacy 6	
Pharmacy 7	
Pharmacy 8	
Pharmacy 9	Google
Pharmacy 10	
Pharmacy 11	Google, Pingdom
Pharmacy 12	Facebook, Google, Pingdom
Pharmacy 13	Pingdom
Pharmacy 14	Pingdom
Pharmacy 15	Google, Pingdom
Pharmacy 16	Google, Pingdom
Pharmacy 17	Google
Pharmacy 18	Giosg, Google
Pharmacy 19	Google, Hotjar
Pharmacy 20	

However, the most interesting and sensitive information sent out to third parties concerns the customer (identified by an IP address or a device identifier) visiting the product page of a specific prescription medicine, or visiting the prescription medicine order page. The former of these indicates interest in a specific medicine and the latter indicates that the customer intends to place an order. These alone are personal data items that should not be sent to third parties. When the customer's visit on a product page of a specific prescription

medicine can be connected to an order by the same customer (indicating an intention to order a specific medicine) and this data is sent to a third party, a strong argument can be made that sensitive health related data is being leaked.

The aforementioned connection between a specific medicine and an order can be strong or weak. The strong connection is formed when the previously visited page (referer) is sent to the third party when the customer is on the prescription medicine order page. This way, the third party can immediately see that the order has been initiated from a product page of a specific medicine, which indicates the intent of ordering the prescription medicine in question. Often the medicine name was even contained in the product page's URL address. The weaker connection is created when the previously visited page is not directly sent to a third party, but both the product page of a medicine and the order page include analytics from the same third party. The third party can now see from timestamps that these pages have been visited consecutively and deduce that an order for a specific medicine is likely being placed. In both of these cases, the third party can say with great certainty that the customer intends to order a specific prescription medicine, although the weaker connection requires more analysis.

Table 2. The data items related to viewing and ordering prescription medicines delivered to analytics services.

	Website had analytics	Data on specific medicine being viewed is sent to 3rd party	Data on intent to make order is sent to 3rd party	Intent to order can be connected to specific medicine
Pharmacy 1	X	X	X	X
Pharmacy 2	X	X	X	X
Pharmacy 3	X	X	X	X
Pharmacy 4	X	X	X	X
Pharmacy 5				
Pharmacy 6				
Pharmacy 7				
Pharmacy 8				
Pharmacy 9	X	X	X	X
Pharmacy 10				
Pharmacy 11	X		X	
Pharmacy 12	X		X	
Pharmacy 13	X		X	
Pharmacy 14	X		X	
Pharmacy 15	X		X	
Pharmacy 16	X		X	
Pharmacy 17	X		X	
Pharmacy 18	X	X	X	X
Pharmacy 19	X	X	X	X
Pharmacy 20				

Table 2 shows what kind of information about the user's actions is delivered to the analytics providers from each studied pharmacy website. The first column indicates whether the online pharmacy in question had any third-party analytics. The second column designates whether the information about the user viewing a specific medicine's product page is sent to the analytics providers. The third column indicates whether the intent to make an order was leaked. Finally, the fourth column shows whether the intent to order can be linked to a specific medicine.

We can see that in 7 cases, the intent to order a specific medicine was leaked to one or more third-party analytics providers. Altogether, the intent to make an order was leaked in 14 cases, although 7 of these leaks did not have information on the ordered medicine. Although the sample of 20 online pharmacies is not a very large dataset, it is definitely an alarming observation that 14 pharmacies were leaking information about sensitive medicine orders and 7 of these pharmacies revealed the exact prescription medicine a specific user intended to order to third parties.

The different colors in Table 2 indicate different platforms used to build the pharmacy websites. The first platform, marked in red, is a platform used for many different web stores, not only online pharmacies. It has an easy option to integrate Google Analytics to the web store, for example. However, half of the pharmacies built with Platform 1 have chosen not use any analytics. Platform 2, shown in green, is a Finnish specifically built for online pharmacies. Nevertheless, analytics are used on every website built on this platform. It it noteworthy, however, that on websites built with Platform 2, information on a specific medicine was never sent to analytics services. Finally, Platform 3, in blue, is also a Finnish solution for online pharmacies, emphasizing both use of analytics and security in its advertising. Judging from Pharmacies 17–19, these two goals seem to be in conflict when it comes to practice.

Table 3 shows the information privacy policies contained about delivering sensitive health related data to third parties. The table contains only those 16 online pharmacies that were found to have analytics on their websites. We can see that 10 out of 16 pharmacy websites denied sending any data about medicines or products users have displayed or ordered, although our network traffic analysis clearly proves this happens. Three studied pharmacies admitted that this information can be shared with third parties, although they did not explicitly state that information about intended prescription medicine orders is being sent out. The used language was more subtle, stating that the collected personal data, among many other personal data items, includes information on ordered products. In another section of the privacy policy, it was then stated that personal data can be shared with third parties. One of the privacy policies (Pharmacy 17) did not clearly indicate whether personal data is given to third parties. It is also worth noting that Pharmacy 1 explicitly stated in its cookie consent banner that information about prescriptions or medication is not collected.

It is clear that pharmacies did not adequately inform the users about the fact that sensitive health related data is turned over to third parties. It was

Table 3. The information privacy policies contained about delivering sensitive medical data to third parties. The table only contains pharmacies that had analytics on their websites.

	Mention about medicine orders being delivered to 3rd parties	Mention about medicine orders NOT being sent to 3rd parties
Pharmacy 1		X
Pharmacy 2		X
Pharmacy 3	X	
Pharmacy 4	X	
Pharmacy 9	X	
Pharmacy 11		X
Pharmacy 12		X
Pharmacy 13		X
Pharmacy 14		X
Pharmacy 15		X
Pharmacy 16		X
Pharmacy 17		
Pharmacy 18		X
Pharmacy 19		X

also evident in many cases that a privacy policy document had been directly copied from another online pharmacy without sufficiently paying attention to their contents and applicability to the online pharmacy in question. Several privacy policies – or at least large sections of the documents – were identical with each other, even sharing the same spelling mistakes on several occasions.

5 Discussion

Our results have showed that the current state of data privacy in Finnish online pharmacies gives reason for great concern. Sensitive information such as data revealing a person's intention to order prescription medicine should be granted special protection. Also, in many cases this data can be further used to deduce what diseases a person is suffering from. This is especially the case when several medicines are ordered or when the third-party analytics service has an opportunity to observe numerous orders over time, revealing details on a person's medical history. It is clear this information should not be disclosed to third parties. It is also possible that analytics services end up collecting information of an intention to purchase medicine which does not result in ordering the medicine in question due to intervention from the pharmacist. Thus, the collected data can also lead into misinterpretations about the person's health status.

In most cases, the health related data and the third-party analytics companies receiving the data were not mentioned in privacy policy documents. Even if the collection and sharing of data would be transparent, in this context transferring

data concerning intention to order prescription medicines to a third party can be considered highly unethical and unnecessary [16].

In this study, we only covered a subset of all Finnish online pharmacies. Judging from the numbers of online pharmacies with serious privacy problems in this subset, however, it is likely that there are dozens of more pharmacy websites that leak health related data to third parties. Therefore, it is safe to say that the problem is much bigger, both in Finland and in other countries. While it is impossible to say whether the analytics providers really store and use the health related data they receive or whether it is discarded, it is unacceptable that data is sent out to begin with. It is important to note, however, that the leaked data about intended prescription medicine orders only goes to analytics service providers who do not necessarily have an incentive to use it further, and the data likely does not end up in open data market. Making use of the data would probably also require some manual work and additional knowledge about how the specific online pharmacy is implemented in many cases.

The software platforms' developers use to build online pharmacy websites are a significant factor contributing to the privacy problem. These platforms often readily offer the option to effortlessly deploy and turn on third-party analytics services, which makes it easy to enable analytics without fully appreciating the consequences. While letting health related data leak to third parties may often be unintentional, in the case of online pharmacies the implications can be very serious. It may not immediately occur to developers that in terms of privacy, an online pharmacy should not be treated like an average web store. Software developers and data protection officers should pay more attention to what kind of data flows out from their websites. This is easy to accomplish with a similar setup as the one used in this study. Such data flow analysis should always be an integral part of the web development and testing process. The privacy practises of the used platforms should be carefully assessed and analytics should not be used on pages which reveal vulnerable aspects of users. If analytics are deemed necessary, the data should be stored locally by the pharmacy (e.g. using open source analytics solutions such as Matomo [5]), not delivered to a third party.

It is also obvious from our results that online pharmacies have failed to write clear and truthful privacy policies, which is unfortunately a common problem in today's web services [11]. The analyzed privacy policy documents do not provide appropriate information about processing activities. Following a small number of standardized templates when composing privacy policy documents would make them easier to produce and understand [14].

Finally, it is worth noting that our study also aims to have a societal impact by making the results available for online pharmacies so that data leaks can be fixed and unnecessary analytics services are removed from critical pages. As a result of this study, Pharmacy 1 has already removed analytics services from its website, revamped its privacy policy, and reconsidered its privacy practices. We have also reported our findings on other online pharmacies, which will hopefully also help to improve privacy on their websites.

6 Conclusions

We have presented a study of data leaks on Finnish pharmacy websites. We found that out of 20 studied online pharmacies, 14 pharmacies were leaking information about prescription medicine orders, and 7 of these pharmacies revealed to third parties the exact prescription medicine a specific user intended to order. Although the sample is relatively small, the result that 70% of the studied is pharmacies leak health related personal data is highly concerning.

Our findings warrant more research with a wider data set, and we are already in the process of extending this study to cover all Finnish online pharmacies. In the future, online pharmacies in other countries should also be studied in the same manner. Data leaks could also be further studied by experimenting with different consent choices on pharmacy websites.

We also hope that these results are a wake-up call for software developers and data protection officers involved in maintaining essential services that involve sensitive data. It is vitally important for service operators to understand their accountability for protecting customer's privacy in areas where they are particularly vulnerable, including raised awareness and control over the used online platforms and the related design choices. At the same time, users should be clearly informed of what personal data is processed and which parties process it. When it comes to pharmacy websites, the use of any external analytics service, let alone several of them, is difficult to justify. Customers should be able to trust online pharmacies just as much as they trust traditional brick-and-mortar pharmacies.

Acknowledgements

This research has been funded by Academy of Finland project 327397, IDA – Intimacy in Data-Driven Culture.

References

1. Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779, paragraph 49.
2. Almeida, F., Santos, J.D., Monteiro, J.A.: The challenges and opportunities in the digitalization of companies in a post-covid-19 world. IEEE Engineering Management Review **48**(3), 97–103 (2020)
3. Article 29 Data Protection Working Party: Opinion 4/2007 on the concept of personal data. adopted on 20th june. wp 136, p. 4.
4. Bygrave, L., Tosoni, L.: Article 4(1). personal data. In: Kuner, C., Bygrave, L., Docksey, C., Drechsler, L. (eds.) The EU General Data Protection Regulation: A Commentary. Oxford University Press, Oxford, United Kingdom (2020)
5. Gamalielsson, J., Lundell, B., Butler, S., Brax, C., Persson, T., Mattsson, A., Gustavsson, T., Feist, J., Lönroth, E.: Towards open government through open source software for web analytics: The case of matomo. JeDEM-eJournal of eDemocracy and Open Government **13**(2), 133–153 (2021)

6. Heino, T., Carlsson, R., Rauti, S., Leppänen, V.: Assessing discrepancies between network traffic and privacy policies of public sector web services. In: Proceedings of the 17th International Conference on Availability, Reliability and Security. pp. 1–6 (2022)
7. Huo, M., Bland, M., Levchenko, K.: All eyes on me: Inside third party trackers' exfiltration of phi from healthcare providers' online systems. In: Proceedings of the 21st Workshop on Privacy in the Electronic Society. pp. 197–211 (2022)
8. Linardon, J., Rosato, J., Messer, M.: Break binge eating: Reach, engagement, and user profile of an internet-based psychoeducational and self-help platform for eating disorders. International Journal of Eating Disorders **53**(10), 1719–1728 (2020)
9. Liu, Y., Song, H.H., Bermudez, I., Mislove, A., Baldi, M., Tongaonkar, A.: Identifying personal information in internet traffic. In: Proceedings of the 2015 ACM on Conference on Online Social Networks. p. 59–70. COSN '15, Association for Computing Machinery, New York, NY, USA (2015). https://doi.org/10.1145/2817946.2817947, https://doi.org/10.1145/2817946.2817947
10. Martínez, D., Calle, E., Jové, A., Pérez-Solà, C.: Web-tracking compliance: websites' level of confidence in the use of information-gathering technologies. Computers & Security **122**, 102873 (2022)
11. Mulder, T.: Health apps, their privacy policies and the gdpr. European Journal of Law and Technology (2019)
12. Purtova, N.: The law of everything. board concept of personal data and future of eu data protection law. Innovation and Technology **10**(1), 40–81 (2018)
13. Quintel, D., Wilson, R.: Analytics and privacy. Information Technology and Libraries **39**(3) (2020)
14. Rowan, M., Dehlinger, J.: A privacy policy comparison of health and fitness related mobile applications. Procedia Computer Science **37**, 348–355 (2014)
15. Santin, O., McShane, T., Hudson, P., Prue, G.: Using a six-step co-design model to develop and test a peer-led web-based resource (plwr) to support informal carers of cancer patients. Psycho-oncology **28**(3), 518–524 (2019)
16. Schwartz, P.M.: Privacy, ethics, and analytics. IEEE security & privacy **9**(3), 66–69 (2011)
17. Somenahalli, S., Shipton, M.: Examining the distribution of the elderly and accessibility to essential services. Procedia-social and behavioral sciences **104**, 942–951 (2013)
18. Thompson, N., Ravindran, R., Nicosia, S.: Government data does not mean data governance: Lessons learned from a public sector application audit. Government information quarterly **32**(3), 316–322 (2015)
19. Wambach, T., Bräunlich, K.: The evolution of third-party web tracking. In: Camp, O., Furnell, S., Mori, P. (eds.) Information Systems Security and Privacy. pp. 130–147. Springer International Publishing (2017)
20. Zheutlin, A.R., Niforatos, J.D., Sussman, J.B.: Data-tracking among digital pharmacies. Annals of Pharmacotherapy p. 10600280211061757 (2022)
21. Zheutlin, A.R., Niforatos, J.D., Sussman, J.B.: Data-tracking on government, nonprofit, and commercial health-related websites. Journal of general internal medicine **37**(5), 1315–1317 (2022)