A Study of Third-Party Tracking on Religious Websites

Henna Lohi, Sampsa Rauti, Panu Puhtila, Timi Heino, Sammani Rajapaksha
Department of Computing
University of Turku
Turku, Finland
e-mail: {hmlohi | sjprau | papuht | tdhein | syraja}@utu.fi

***Abstract*—Websites give many advantages to a religious community, making religious practices more accessible and enabling communication and community-building. At the same time, the user's privacy needs to be protected. This is particularly true for the data about their religious beliefs. The General Data Protection Regulation has strict requirements on the processing of special categories of personal data, including data revealing an individual's religious beliefs. This paper presents a case study of websites of the largest religious community in Finland, the Evangelical Lutheran Church. We study the prevalence of third parties and potential data leaks on 31 websites of this church. Our findings show that several measures have been taken to protect the user's privacy by the church and website maintainers, such as introducing a common platform for the vast majority of the websites and replacing Google Analytics with Matomo. However, there were still some privacy concerns such as leaking data to Meta and vague privacy policies. This case study serves both as an example of how many correct measures have been taken to prevent privacy violations and how web developers and data protection officers can further improve data protection.**

Keywords-Third parties; web analytics; data leaks; religious websites; online privacy.

I. Introduction

The information and communication technology is used to deliver all kinds of services and information today. This also goes for religious communities that seek to improve communication, community building and the accessibility of religious practices [1]. Web-based services, in particular, help religious communities to easily share their beliefs and announce events online. This way, they can spread their message, teachings and practices to a wider audience [2][3]. Internet makes it possible for religious communities to extend their reach beyond physical boundaries [4]. The websites of religious communities benefit both current members and those interested in learning more about the religion or community.

Religious beliefs – at least in the largely secular academic world and in postmodernism – are usually regarded as private matters [5]. An argument can be made that this privacy should also extend to online spaces [6]. The General Data Protection Regulation (GDPR) also reinforces this idea, setting strict requirements on the processing of data concerning religious beliefs [7]. Processing such data is forbidden by default, and requires explicit consent or specific legal grounds to occur. Therefore, privacy is an important consideration and challenge when designing websites of religious communities. For example, modern websites often use third-party analytics services. The data collection carried out by these services can lead to the inadvertent disclosure of users' religious affiliations. Protecting sensitive personal data on religious websites requires special attention and care.

In this paper, we study what kinds of third-party services are used on 31 websites of the Evangelical Lutheran Church of Finland. We also examine whether sensitive data concerning users' religious beliefs is sent to third parties. By analyzing the outgoing network traffic generated when browsing the websites, we study whether these websites leak sensitive personal data to third parties. Additionally, we analyze whether the user is into accepting cookies and data collection with dark patterns and whether the user is adequately informed about potential data sharing occurring on these websites. Finally, we also gauge how well the church supports parishes in building websites that prioritize privacy by design.

The rest of the paper is structured as follows. Section II presents the prior work related to our study. Section III explains the study setting and methods. Section IV presents the results of our network traffic analysis, along with an assessment of dark patterns and privacy policies. Section V discusses the lessons learned from assessing the privacy of the studied religious websites and explores the implications of our findings. Finally, Section VI concludes the paper.

II. Related Work

The body of literature on third-party tracking is large. The excessive and intrusive collection of sensitive data has generally been considered a problem [8]–[11] and only rarely a benefit to users [12]. In particular, third-party health data leaks have been widely covered in prior work [13]–[17]. Automatic tools have been build to detect third-party data leaks and assess website privacy [18][19]. Several studies also examine privacy policy documents and gauge how well users are informed of ongoing data collection [20]–[26]. While the topic of data collection and data leaks on websites has been explored widely in the research literature, it has not been studied very extensively in the context of religious websites.

Hoy et al. [27] studied the privacy violations happening in 102 USA-based websites of Christian parishes, and also presented a questionnaire to the parish leadership figures which prompted responses from 23% of them. The sample material of this study consisted of a mixture of different Christian nomination websites, including Lutherans, Methodists, Catholics and Baptists. Their results indicated that as many as 99% of the church websites collected personal identifying information. However, it must be noted that their research methodology was different from ours, as they focused much

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

more on the information that the parishioners knowingly and willingly submitted to the websites, whereas we focus entirely on the use of website analytical tools to collect data.

Samarasinghe et al. [6] conducted a very large scale survey on religious websites from four major religions – Christianity, Buddhism, Islam and Hinduism – focusing on their cybersecurity and privacy aspects. This study was done by utilizing OpenWPM, which is an automated system for detection privacy violations developed by researcher Steven Englehardt [28], Uniform Resource Locator (URL) Classification which is web-based system used for categorization of websites, and VirusTotal, which is a web-based computer virus detection platform operated by Chronicle, a subsidiary of Google. With this technology, Samarasinghe et al. scanned 583 784 websites and ultimately chose 62 373 of them to be analyzed. Their results indicated, among other things, that 27.9% of the religious websites used tracking scripts, and 5.7% used tracking cookies to collect personal data on their users.

While our sample size is small compared to Samarasinghe et al., their methodology was also very different, and that the study of data leaks was only one aspect of their research. Their sample material also consisted of a much more heterogeneous material, comprising websites representing many different religious worldviews and organizations. In contrast, the current study focuses on a very specific religious online presence, the Lutheran parish and diocese websites operating in Finland, presenting multi-case study that delves deeper into a specific group of religious websites. Thus, while their study gives a wider perspective on the privacy behavior of the religious websites in general, ours offers detailed description of websites of one religious community, offering a more in-depth analysis of the privacy issues, third parties and data leaks.

III. Study Setting and Method

In this section, we explain how the study is conducted including the data sets selected, the methods used and the study scope.

A. Case and Website Selection

The Evangelical Lutheran Church of Finland was chosen to be studied because it has a strong connection with the state and is a large organization with hundreds of websites [29]. These include websites for parishes and dioceses around Finland and general websites of the church. The Evangelical Lutheran Church of Finland holds a special legal position as a national church (along with the Orthodox Church of Finland), and has the capability to tax its members. In 2023, over 3.5 million Finns belonged to the Evangelical Lutheran Church. This means that approximately 65.1% of Finns were members of the church. Because of the church's special role and large number of potential visitors, special attention should be paid to the privacy of the church's websites, and it was a logical choice for a multi-case study.

Altogether, the Evangelical Lutheran Church of Finland has 354 local parishes in 9 dioceses [30]. The set of websites to be studied was selected according to the following selection criteria:

- Two parish websites were chosen randomly from each diocese to have a diverse selection of websites from around the country.
- The websites of all 9 dioceses were also selected.
- All the parish websites that did not use the church's own web platform (Lukkari) were also included. As standalone websites, these were deemed more likely to include unique third parties and potential data leaks.
- The general top-level website of the church (evl.fi) was also included in the study.

Overall, 31 websites were chosen to be studied, 17 of which used the Lukkari platform. Because we are first and foremost studying data leaks as a phenomenon here, naming specific parishes or dioceses behind the websites serves no purpose. When necessary, the studied websites are referred to using pseudonyms WS1–WS31.

B. Recording the Network Traffic

Network traffic was recorded with Google Chrome Developer Tools, and saved in HAR (shorthand for HTTP Archive) log files. Upon entering the website, all caches were disabled to ensure that they would not disrupt the recording results. Also, all cookies were consented to. Initially, we accessed the landing page. Following this, we conducted a search using the search feature, if available, and examined other pages on the website, particularly those that might process sensitive personal data or reveal information about how the user practices religion.

All network traffic generated while navigating the website was recorded to determine whether there were any data leaks to third parties and to analyze the nature of this data. Only the HTTP requests directed to third parties (external domains outside the studied web service) were filtered for further inspection. We manually looked through each of the filtered requests to examine the payloads for leaks of sensitive personal data.

Because this study focuses on *personal data*, it is important to define it. According to GDPR and the Finnish Office of the Data Protection Ombudsman, "personal data" refers to "all data related to an identified or identifiable person" [31] [32]. This definition covers technical details like Internet Protocol (IP) addresses, device identifiers, location data, or any variable that helps to identify the user of the website. While all of these data items alone may not identify an individual, they can often be combined to make identification possible, and therefore fall under the definition of "personal data". Rather than the actual identifying data, however, in this study we focused on contextual data related to an identifiable person, most notably religious beliefs.

C. Analyzing the Recorded Network Traffic

When studying the recorded network traffic, we looked for the following two sensitive data leak types in the HTTP request payloads:

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

1) *Search terms*. Search terms are inputs that are usually freely decided by the user, so they can be sensitive. For example, on a parish's website, a user might search information about services held in that parish. This implies interest in ecclesiastic activities and may disclose religious beliefs.
2) *Page URLs*. The individual pages under the website can often reveal specific religious topics the user is interested in. Particularly, numerous different events, such as church services, may have their own separate pages within the website. This way, the religious beliefs and practices to which an individual adheres can be disclosed.

D. Dark Patterns and Privacy Policies

We also analyzed dark patterns, privacy policies and cookie consent banners found on the websites. Dark patterns, UI designs crafted to manipulate users into taking actions they might not otherwise choose, can cause users to inadvertently accept data collection. In this study, we specifically looked at three dark patterns, adapted from the "Report of the work undertaken by the Cookie Banner Taskforce" by European Data Protection Board [33]: 1) The first layer of the cookie consent banner does not offer a reject button, 2) pre-ticked boxes are present in the cookie banner or cookies settings, which can used to define cookie choices, and 3) The "Accept all" button is unfairly highlighted with color or contrast choices in order to attract users to click it.

Privacy policies and cookie consent banners available on the studied religious websites were examined to answer the following questions:

- Does the document clearly inform users that they can be uniquely identified as a result of data collection?
- Does the document clearly mention what personal data items are sent to third parties?
- Does the document name all the third parties receiving the user's personal data?
- Does the document mention that religious beliefs can be revealed as a result of sharing data?

IV. Results

This section exemplifies the results we collected using the above mentioned study methods and data.

A. The General Picture

When it comes to privacy of public sector websites in Finland, the Finnish Deputy Data Protection Ombudsman has stated that governmental agencies must "carefully consider what types of tracking technologies are necessary on their websites." Furthermore, developers of public sector websites should ensure that users are "able to use online services provided by authorities without data on their website visit ending up in commercial use, for example." [34] This statement from the Deputy Data Protection Ombudsman offers clear guidance on how to maintain balance between using tracking technologies and protecting user privacy.

The Evangelical Lutheran Church of Finland has improved the privacy of their websites as a result of the statement. The vast majority of all websites of the church use the common Lukkari platform [35], and Google Analytics formerly employed by this platform was replaced with Matomo in 2023 [36]. Although Google Analytics was widely used by church websites before this, the privacy has since been greatly improved, and the common platform serves to enforce robust privacy.

B. Network Traffic Analysis

Figure 1 represents the most serious leak types we detected: page URL and search term leaks in the 31 studied websites of the Evangelical Lutheran church. On the left, numbers represent the total data leaks (both page URL leaks and search term leaks) for each website. In the middle, data leaks are categorized into two categories, page URL leaks and search term leaks. On the right, the number of data leaks received by each third party is shown. As can be seen, page URL leaks occurred 16 times, and search term leaks 14 times. The recipients of the leaked data were Google, Meta and Siteimprove. It is not surprising that Google Analytics amounted to 50% of all page URL and search term leaks, as it has been proven to be the largest reason for tracking and data leaks happening in websites [37][6]. In the current study, however, Meta amounted only to 3 data leaks, while Siteimprove Analytics, a much smaller analytics provider, amounted to 12 leaks. The reason for this is that the websites did not use Meta's actual analytics service (Meta Pixel) but made use of social media plugins on the websites.

In total, only 12/31 (38.7%) of the studied websites exhibited leaks, which can be seen as a good result, especially considering we intentionally chose to include several websites more likely to contain data leaks in our data set, that is, websites not using the church's Lukkari platform. On average, the websites which did leak data had 2.5 data leaks per website, with the lowest number of leaks being 1 and the highest being 4.

It must be noted that there were some third parties that were not considered risky and thus not counted in data leaks. Firstly, the Matomo analytics service, which allows the website maintainer to retain the control over the data (although data may be stored on a remote server), was not counted. Rather than a harmful analytics service, it is a recommended service. Giosg, a popular chat service based in Finland was also not counted as a risky third party. Finally, Snoobi, a Finnish analytics service also widely used by public sector and state websites, was also excluded.

Matomo was found on 24/31 (77.4%) websites, which is a good result from privacy point of view. However, on many websites it was used along with other analytics services, which greatly undermines its privacy benefits. Still, compared to many other studies [37][38], the number of third parties (3) receiving sensitive data is exceptionally small, which speaks of decent privacy practices.

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

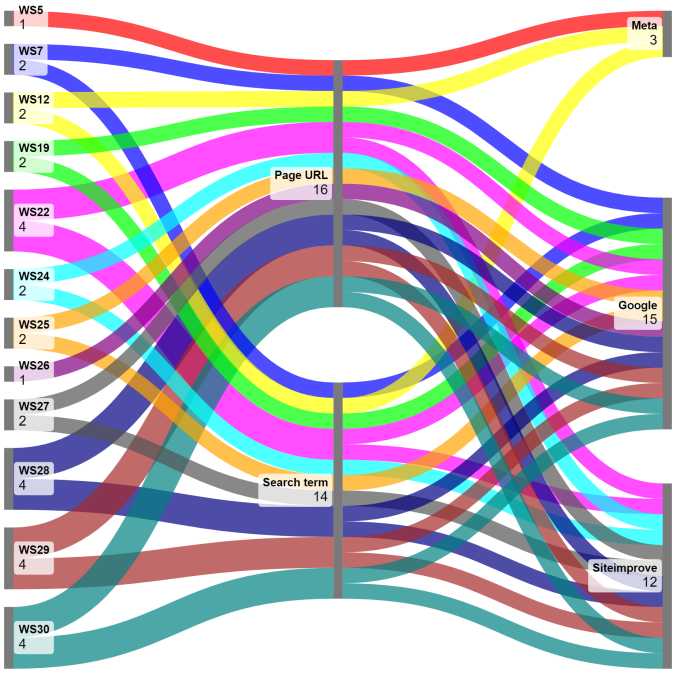

Figure 1. Data leaks detected on 12 different websites.

It is also worth noting that although not considered a highly serious data leak type here and not included in Figure 1, there were also website URL leaks in the studied pages. Although not as critical as the page URL and search term leaks discussed above, website URLs reveal that the user has visited a specific website (domain name). They do not give information on visiting specific subpages, but regular visits to the same website could still reveal the user's religious affiliation. The studied websites leaked the website URL to Meta 10 times, to Google 8 times and to Siteimprove 6 times. Finally, it is worth noting that there was also one third party, X/Twitter, which was present on more than half (16) of the studied websites as a social media plugin, but never received sensitive personal data such as visited pages.

Lastly, what makes the data leaks discussed here sensitive is the combination of identifying data (such as an IP address) and contextual data (such as a URL of a visited page). There are several reasons why an individual user can often be uniquely identified by third parties. First off, an IP address is a crucial piece of data for identifying users [39] and it is considered personal data in most cases [31]. Third parties can also identify users through cookies. For example, Google Analytics uses a cookie that lasts for 2 years and includes a unique client ID (cid) to distinguish users [40]. Google also uses cross-device tracking by leveraging data from logged-in Google accounts [41]. Similarly, Meta/Facebook uses accounts to keep track of users using different devices. Because of these technologies, users' actions and the pages they visit are not just linked to IP addresses, but in many cases, to actual names of individual persons.

C. Privacy Policies, Cookie Consent Banners and Dark Patterns

There were 4 websites that failed to name the third parties in their privacy policies or cookies consent banners, even though our network traffic analysis showed they had third parties present. Other 25 websites that had third parties present did mention these third parties either in their privacy policies or cookie consent banners, which is a positive result. However, we found that none of the websites collecting data informed the user adequately of the possibility of unique identification. Also, none of the privacy policies or cookie consent banners clearly mentioned that visited URLs or search terms are shared to third parties, even when this was often the case in reality. However, 8 websites vaguely mentioned collecting data on how the visitors use the website. Lastly, the possibility of religious beliefs leaking was never mentioned.

Privacy policies and cookie consent banners of all studied websites of the parishes were identical with each other, and those used by the dioceses except one were identical with each other. In other words, the parishes used one kind of template for these elements, and dioceses used another. However, the third parties the websites included varied.

In many sections of the privacy policies of the diocese websites, the possibility of data collection was explained in raw technical details that are difficult for the average website users to comprehend. This issue of privacy policies containing overly technical jargon has been recognized in prior research [42]. Also, many categorizations of the data collection methods were incorrect or highly ambiguous.

Privacy policies of the parishes, on the other hand, all linked to the same website containing the privacy policy, maintained by the Evangelical Lutheran Church of Finland [43]. This website listed all of the third parties present, and provided a short common language explanation for the cookies in use. However, it provided the details of the cookies used by linking to other websites, which were maintained by the proprietors of these analytics services. Most of these websites were in English, and all of them asked for permission to data collection, which can be seen as highly problematic in its own right. This forces the user to enter a third-party website and make a decision whether to allow the web analytics on that website to harvest their data, just to read how the cookies are used on the original parish website.

Out of 31 websites, 5 (16.1%) did not ask for consent for cookies and data collection at all, although they collected personal data. As a positive result, the rest of the studied cookie consent banners did offer a reject button on the first layer, and none of the banners had pre-ticked selection boxes. On 9 websites (29.0%), however, the cookie consent banners unfairly highlighted the accept button with prominent colors and contrast. It must be noted that the reject button was always labeled as "Allow only necessary", which could be considered slightly misleading. Also, the tickable consent boxes used in the cookie consent banners were colored light gray when the consent had been given, and black when not. This can be

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

considered misleading since the usual convention is to use a lighter color for unchecked boxes and a darker color when it is checked. In essence, the common convention of using colors in website design was inverted in these banners.

V. Discussion

The results are further discussed in this section. The main discussion points are given as subsections.

A. Lessons Learned in Web Development

There are many lessons to be learned from the studied websites and their privacy practices. In what follows, we will explore both positive and negative aspects based on our findings.

1) Positive Aspects:

Following the privacy guidelines. The Evangelical Lutheran Church of Finland, unlike many other public sector bodies, has taken note of the Deputy Data Protection Ombudsman's statement on the use of third parties on the websites of public sector bodies and the careful consideration of necessary tracking technologies. This shows that guidelines and recommendations by data protection authorities have a significant effect on privacy in practice. While our findings and lessons learned are applicable to other religious communities in many respects, it is very likely that not all communities have followed privacy recommendations equally well. The same can be said of many other application areas, such as healthcare, where web-based systems often seem to lack much needed privacy measures.

Common platform and clear recommendations. The vast majority of the websites are using the same platform and the church strongly advocates employing a local analytics solution, Matomo, instead of Google Analytics. Matomo enables the church to control the collected data without sharing users' personal data with third parties [44][45]. Therefore, it is evident that although using a common platform can sometimes have negative effects to privacy by introducing or making it easy to include third-party analytics [46], it can also prevent data leaks when done correctly.

Getting rid of Google Analytics. Taking advantage of the commonly used platform, the church has systematically phased out Google Analytics, which has been seen to be a problematic (and even illegal) web analytics solution based on the Deputy Data Protection Ombudsman's statement.

Migrating away from third-party analytics. The case of Evangelical Lutheran Church of Finland also demonstrates that data collected with Google Analytics can be migrated to Matomo, even though it is not a quick and entirely straightforward process, when there is lots of gathered data.

Using a small set of third-party services. The church websites only made use of a very small number of third-party services, and data only leaked to 3 third parties. This makes it possible to scrutinize the used services more closely and improves user privacy.

2) Issues to be Addressed:

Not consistently using the common platform and failing to follow recommendations. Some of the parish websites did not use the provided Lukkari platform, even though it has been available for about 10 years. Moreover, some of the websites not built with the platform still used Google Analytics, although its use is discouraged both by the church and data protection authorities.

Ignoring risky third parties Another problem is ignoring privacy issues caused by certain third parties even when the common platform is used. Most notably, URL addresses of visited pages leaked to Meta on two websites using the Lukkari platform. It can be argued that Meta is as problematic a data collector as Google is. Earlier studies have suggested that Meta has commercially exploited potentially sensitive personal data for advertising purposes [47]. From this viewpoint, we argue it is quite obvious that the previously mentioned Deputy Data Protection Ombudsman's statement should also be applied to Meta and Meta's services should not be used on pages processing sensitive data if they leak the page URL.

Vague privacy policies. All the studied websites used privacy policy documents that were generic and unclear at many points. For example, as the third parties used on the websites vary, privacy policies should also reflect this by clearly mentioning the used third-party services. Users should be able to find out what kind of personal data is being sent out and to which third parties it is being shared. The privacy policies should mention that the visited pages and their topics can leak to third parties, some of which may be processing data outside of Europe.

Inadequate consent. Not all websites asked for consent for cookies and data collection. This violates the GDPR when the website uses cookies [48]. Leaking data concerning religious beliefs is especially serious when no consent is asked. Even when a general consent for data collection was requested, data concerning religious beliefs was never specifically mentioned and it is unlikely the user expects this kind of information to be shared with third parties.

B. Implications for Users

When a website leaks a user's religious affiliation to a third party, the user's privacy is violated. The user's personal beliefs are shared and revealed, often without their explicit permission. As a result of this, users may feel they have lost control over their personal information. The leaked data concerning religion can be used in targeted advertising or attempts to persuade people [49]. It is possible that some actors might try to change a person's religious or political views based on the gathered data. Obviously, these kinds of actions raise ethical concerns and go against an individual's right to make their own choices.

In certain societies, people might face prejudice or unfair treatment due to their faith when others find out about it [50]–[52]. This unfair treatment can manifest in different ways, like being left out or not getting hired for jobs. In extreme cases,

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

sensitive religious data leaked could even put people at risk if malicious actors get their hands on it. While this may be unlikely, the simple fact that these possible dangers exist is enough reason to prevent careless sharing of sensitive personal data.

Website visitors may also stop trusting their religious group if their sensitive personal data is leaked to third parties. This can hurt relationships between community members and make them doubt their leaders. Moreover, leaking an individual's religious beliefs can cause them a lot of pain and anxiety. Religious communities that let such data fall into wrong hands could also face legal problems.

VI. Conclusion

To conclude, findings of this study are promising in regards to user privacy. The number of third parties and privacy issues detected was relatively small when compared to other studies and categories of websites [6][37]. This is mainly the result of the Evangelical Lutheran Church of Finland having an organization-wide policy of using the same platform for the majority of their websites, which significantly reduces the number of third-party services in use. While using a common platform does not always result in a positive outcome, in this particular case it has resulted in uniform adoption of stringent privacy practices, which can in many ways be considered a recommendable outcome.

Still, several websites were found to leak personal data potentially revealing the user's religious beliefs to third parties such as Google and Meta. This was because all websites did not use the common Lukkari platform provided by the church but also because this platform still allowed third parties like Meta and Siteimprove to be present. This is why an external privacy audit would still be a good idea for the websites processing sensitive data like religious beliefs. Avoiding dark patterns and aiming for the clarity and comprehensiveness of privacy policies are also areas where corners can not be cut. As future work, we plan to extend this examination to other religious communities.

Acknowledgments

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

References

[1] O. Golan and N. Stadler, "Building the sacred community online: The dual use of the internet by chabad," *Media, culture & society*, vol. 38, no. 1, pp. 71–88, 2016.

[2] P. H. Cheong, J. P. Poon, S. Huang, and I. Casas, "The internet highway and religious communities: Mapping and contesting spaces in religion-online," *The Information Society*, vol. 25, no. 5, pp. 291–302, 2009.

[3] T. Hutchings, "Contemporary religious community and the online church," *Information, Communication & Society*, vol. 14, no. 8, pp. 1118–1135, 2011.

[4] A. Vitullo, "Multisite churches. creating community from the offline to the online," *Online-Heidelberg Journal of Religions on the Internet*, 2019.

[5] D. Shatz, "On Undermining the Beliefs of Others: Religion and the Ethics of Persuasion," *Faith: Jewish Perspectives*, pp. 137–187, 2013.

[6] N. Samarasinghe, P. Kapoor, M. Mannan, and A. Youssef, "No salvation from trackers: Privacy analysis of religious websites and mobile apps," in *International Workshop on Data Privacy Management*, Springer, 2022, pp. 151–166.

[7] GDPR-info.eu, *Processing of special categories of personal data*, https://gdpr-info.eu/art-9-gdpr/, Accessed: 2024-08-22, 2024.

[8] T. Wambach and K. Bräunlich, "The evolution of third-party web tracking," in *Information Systems Security and Privacy: Second International Conference, ICISSP 2016, Rome, Italy, February 19-21, 2016, Revised Selected Papers 2*, Springer, 2017, pp. 130–147.

[9] P. M. Schwartz, "Privacy, ethics, and analytics," *IEEE security & privacy*, vol. 9, no. 3, pp. 66–69, 2011.

[10] A. R. Zheutlin, J. D. Niforatos, and J. B. Sussman, "Data-tracking on government, non-profit, and commercial health-related websites," *Journal of general internal medicine*, pp. 1–3, 2021.

[11] A. Chandler and M. Wallace, "Using Piwik instead of Google analytics at the Cornell university library," *The Serials Librarian*, vol. 71, no. 3-4, pp. 173–179, 2016.

[12] I. Kes, D. Heinrich, and D. M. Woisetschlager, "Behavioral targeting in health care marketing: Uncovering the sunny side of tracking consumers online," in *Let's Get Engaged! Crossing the Threshold of Marketing's Engagement Era: Proceedings of the 2014 Academy of Marketing Science (AMS) Annual Conference*, Springer, 2016, pp. 297–297.

[13] M. D. Huesch, "Privacy threats when seeking online health information," *JAMA Internal Medicine*, vol. 173, no. 19, pp. 1838–1840, 2013.

[14] M. Huo, M. Bland, and K. Levchenko, "All eyes on me: Inside third party trackers' exfiltration of phi from health-care providers' online systems," in *Proceedings of the 21st Workshop on Privacy in the Electronic Society*, ACM, 2022, pp. 197–211.

[15] A. Surani *et al.*, "Security and privacy of digital mental health: An analysis of web services and mobile apps," in *Conference on Data and Applications Security and Privacy*, 2023.

[16] X. Yu, N. Samarasinghe, M. Mannan, and A. Youssef, "Got sick and tracked: Privacy analysis of hospital websites," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, 2022, pp. 278–286.

[17] A. R. Zheutlin, J. D. Niforatos, and J. B. Sussman, "Data-tracking on government, non-profit, and commercial health-related websites," *Journal of general internal medicine*, vol. 37, no. 5, pp. 1315–1317, 2022.

[18] V. Wesselkamp *et al.*, "In-depth technical and legal analysis of tracking on health related websites with ernie extension," in *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, ACM, 2021, pp. 151–166.

[19] R. Carlsson, P. Puhtila, and S. Rauti, *Towards an automatic tool for detecting third-party data leaks on websites*, Accepted to the 10th Workshop on Software Quality Analysis, Monitoring (SQAMIA2023), 2023.

[20] G. P. Dias, H. Gomes, and A. Zúquete, "Privacy policies and practices in portuguese local e-government," *Electronic Government, an International Journal*, vol. 12, no. 4, pp. 301–318, 2016.

[21] K. Schnell and R. Kaushik, "Hunting for the privacy policy – hospital website design," SSRN Elsevier, 2022.

[22] S. D. Brown and Y. Levy, "Towards a development of an index to measure pharmaceutical companies' online privacy practices," *Online Journal of Applied Knowledge Management (OJAKM)*, vol. 1, no. 1, pp. 93–108, 2013.

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

[23] T. Kautto and P. Henttonen, "Availability and findability of FOI and privacy statements on Finnish municipalities' websites," *Tidskriftet Arkiv*, vol. 8, no. 1, 2017.

[24] J. Burkell and A. Fortier, "Privacy policy disclosures of behavioural tracking on consumer health websites," in *Proceedings of the American Society for Information Science and Technology*, vol. 50, Wiley Online Library, 2013, pp. 1–9.

[25] A. Beldad, M. de Jong, and M. Steehouder, "Reading the least read? indicators of users' intention to consult privacy statements on municipal websites," *Government Information Quarterly*, vol. 27, no. 3, pp. 238–244, 2010, ISSN: 0740-624X.

[26] K. Schuele, "Privacy policy statements on municipal websites," *The Journal of Government Financial Management*, vol. 54, no. 2, pp. 20–29, 2005.

[27] M. G. Hoy and J. Phelps, "Consumer privacy and security protection on church web sites: Reasons for concern," *Journal of Public Policy & Marketing*, vol. 22, no. 1, pp. 58–70, 2003.

[28] S. Englehardt, "Automated discovery of privacy violations on the web," Ph.D. dissertation, Princeton, NJ: Princeton University, 2018.

[29] Evangelical Lutheran Church of Finland, *Published websites*, https://lukkariohje.evlut.fi/tietoa-lukkarista/julkaistut, Accessed: 2024-08-22, 2024.

[30] Evangelical Lutheran Church of Finland, *Parishes*, https://evl.fi/en/the-church/organisation/parishes/, Accessed: 2024-08-22, 2024.

[31] Office of the Data Protection Ombudsman, *What is personal data?* https://tietosuoja.fi/en/what-is-personal-data, Accessed: 2024-08-22, 2024.

[32] GDPR.eu, *What is considered personal data under the EU GDPR?* https://gdpr.eu/eu-gdpr-personal-data/, Accessed: 2024-08-22, 2024.

[33] European Data Protection Board, *Report on Work Undertaken by the Cookie Banner Taskforce*, https://edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en, Accessed: 2024-08-22, 2024.

[34] Office of the Data Protection Ombudsman, *Deputy Data Protection Ombudsman Issues Reprimand for Conveying Library Search Information to US-Based Google*, https://tietosuoja.fi/en/-/deputy-data-protection-ombudsman-issues-reprimand-for-conveying-library-search-information-to-us-based-google, Accessed: 2024-08-22, 2024.

[35] Evangelical Lutheran Church of Finland, *Lukkari-ohje*, https://lukkariohje.evlut.fi/, Accessed: 2024-08-22, 2024.

[36] Evangelical Lutheran Church of Finland, *Kävijäanalytiikka*, https://lukkariohje.evlut.fi/yleiset-ohjeet/kavijaanalytiikka, Accessed: 2024-08-22, 2024.

[37] T. Heino, S. Rauti, R. Carlsson, and V. Leppänen, "Study of third-party analytics services on university websites," in *International Conference on Hybrid Intelligent Systems*, Springer, 2022, pp. 1284–1292.

[38] A. Vänskä *et al.*, "Fair data is the new black: Online shopping, data leaks, and broadening the understanding of sustainable fashion," *Fashion Theory*, pp. 1–29, 2024.

[39] V. Mishra *et al.*, "Don't count me out: On the relevance of ip address in the tracking ecosystem," in *Proceedings of The Web Conference 2020*, 2020, pp. 808–815.

[40] Google, *How google uses cookies*, https://policies.google.com/technologies/cookies?hl=en-US, Accessed: 2024-08-22, 2024.

[41] Google, *[GA4] Activate Google signals for Google Analytics 4 properties*, https://support.google.com/analytics/answer/9445345?hl=en, Accessed: 2024-08-22, 2024.

[42] C. D. Asay, "Consumer information privacy and the problems (s) of third-party disclosures," *Nw. J. Tech. & Intell. Prop.*, vol. 11, p. 321, 2012.

[43] Evangelical Lutheran Church of Finland, *Evästeiden käyttö verkkosivuilla*, https://evl.fi/tietosuoja/evasteet/, Accessed: 2024-08-22, 2024.

[44] J. Gamalielsson *et al.*, "Towards open government through open source software for web analytics: The case of matomo," *JeDEM-eJournal of eDemocracy and Open Government*, vol. 13, no. 2, pp. 133–153, 2021.

[45] D. Quintel and R. Wilson, "Analytics and privacy," *Information Technology and Libraries*, vol. 39, no. 3, 2020.

[46] S. Rauti *et al.*, "Analyzing third-party data leaks on online pharmacy websites," *Health and Technology*, pp. 1–18, 2024.

[47] J. G. Cabañas, Á. Cuevas, and R. Cuevas, "Unveiling and quantifying facebook exploitation of sensitive personal data for advertising purposes," in *27th USENIX security symposium (USENIX security 18)*, 2018, pp. 479–495.

[48] T. Wei, C. Cao, and Y. Shi, "Personal information protection behaviors of consumers in different country context and user interface designs," in *International Conference on Human-Computer Interaction*, Springer, 2022, pp. 82–98.

[49] Á. Cuevas, J. G. Cabañas, A. Arrate, and R. Cuevas, "Does facebook use sensitive data for advertising purposes? worldwide analysis and dgpr impact," *arXiv preprint arXiv:1907.10672*, 2019.

[50] J. L. Roberts, "Protecting privacy to prevent discrimination," *Wm. & Mary L. Rev.*, vol. 56, pp. 2097–2175, 2014.

[51] F. A. Whitlock and J. Hynes, "Religious stigmatization: An historical and psychophysiological enquiry," *Psychological Medicine*, vol. 8, no. 2, pp. 185–202, 1978.

[52] V.-I. Savic, "GDPR and Religious Freedoms (With Insight Into Ronald Dworkin and Competing Rights)," *CEJCL*, vol. 3, p. 115, 2022.

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org