Privacy Risks of Third-Party Services on Women's Shelter Websites

Panu Puhtila
Department of Computing
University of Turku
Turku, Finland
papuht@utu.fi

Robin Carlsson
Department of Computing
University of Turku
Turku, Finland
crcarl@utu.fi

Sampsa Rauti
Department of Computing
University of Turku
Turku, Finland
sjprau@utu.fi

***Abstract*—Women's shelters usually operate with a commitment to confidentiality to protect the privacy and safety of the help-seeking individuals. In today's digital age, this principle also extends to their websites, highlighting the importance of online visitors' privacy. This study discusses the potential negative outcomes of using third-party analytics services on websites of the women's shelters, conducted by analyzing the contents of web requests made to third parties and how they jeopardize the user privacy. The results show that 95.5% of the studied websites leak visitors' personal data, such as IP addresses, and device identifiers. Along with these identifying details, the current website URL is also leaked, potentially revealing the user's intent to seek help. Consequently, detailed profiles of violence victims could be created by third parties. The study also offers recommendations to protect the confidential personal data of vulnerable individuals seeking support.**

***Index Terms*—women's shelters, violence shelters, web privacy, third-party services**

I. Introduction

Women's shelters provide services to the people who are, by definition, in an extremely vulnerable position [1]. Shelters usually operate in a confidential and secure manner to protect the privacy and safety of the help-seeking individuals [2]. Many shelters have recognized the importance of online presence and have set up websites to complement their other services. On the shelter websites, victims can find information about the offered services, information on the shelter, counseling, legal support, etc. They may also offer educational materials about domestic violence and safety planning. In recent years, the use of these web services has likely increased as a consequence of the accelerated digitalization and COVID-19 pandemic, which has also raised domestic violence rates [3].

Due to the highly vulnerable and sensitive position of individuals browsing shelter websites, it is paramount that no identifying data about those using the web services of the shelters should be leaked to third parties, as it could potentially have serious and even life-threatening consequences. At the same time, third-party services such as web analytics, chat services and tools used to optimize website performance have become very commonplace on websites. While these services offer multiple benefits in terms of analyzing visitor behavior and assessing quality of websites, their use also raises serious privacy concerns.

There is a large body of research on women's shelters in general, across several academic disciplines [4]–[10] and stretching back decades. However, the specific topic of online privacy and security in the context of these shelters has to our best knowledge not received any attention in the previous scientific research. The current paper is the first one to analyze third-party data leaks on shelter websites, and the confidentiality of these essential web services in general.

The current study focuses on assessing the extent to which women's shelter websites leak data to third parties. To this end, we conduct a network traffic analysis in regards to web requests made to third parties, and infer whether they leak any personal, or otherwise identifiable information to these actors. We also take a look at the cookie banners and privacy policies employed by these web services. We examine whether the cookie banners employ deceptive practices to coax users into accepting cookies and analytics, and assess how well the user is informed about personal data collection.

The rest of the paper is organized as follows. Section II discusses the study setting and the methods used in collecting and analyzing the data. Section III covers the observable results of our research. In section IV, we take a look at possible consequences which may result from our findings, and offer propositions on how to better design women's shelter web services to safeguard their users' privacy. Finally, in Section V, we present the definite conclusions of our study.

II. Study Setting

In this study, we examined the websites of 22 women's shelters. The sites to be studied were chosen from the listing of shelters maintained by the Finnish institute of health and welfare, THL[1]. From this list, we chose the shelters which had a functioning website. One of the studied services, Shelter no. 22, was not on the list, but was chosen as part of the dataset as it was linked to many of the services that were being studied. Of these web services, 11 were hosted on the same domain[2],

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

[1]https://thl.fi/fi/palvelut-ja-asiointi/valtion-sosiaali-ja-terveydenhuollon-erityispalvelut/turvakotipalvelut/turvakodit/turvakotien-yhteystiedot

[2]https://ensijaturvakotienliitto.fi

and the remaining 11 were hosted on their own domains. Many of the sites were part of larger website complexes.

Our experiment involved running a short testing sequence on the selected websites. All cookies were consented to when arriving at the selected websites. We then navigated from the landing page of the web service to the help-seeking page of the shelter in question. If the website had a chat or additional info pages about the shelter in question, these were also accessed. In addition to this, if the site had any collapsible content (elements that can be clicked open) used for info boxes, these were studied as well. Finally, all network traffic generated while navigating the website was recorded to determine whether the website leaks data to third parties, and to analyze the nature of this data. Recording of the traffic was done by Google Chrome's Developer Tools, referred to as devtools from this point on. All recording was done with the cache disabled, so as to ensure that no previously cached data would distort the test results. Using devtools allowed for the examination of the network traffic during the testing sequence. From the recorded data, only the web requests which went to the third parties were filtered for further inspection.

Locations of the servers where the leaked data was sent to were determined by using the `iplocation.net` service, which combines results of eight different location services. Here we have adhered to a principle that if all eight referred services show the same location, then we can be relatively sure that the location is correct. If there was no consensus amongst the location services, we have abstained from naming the location.

All recorded traffic was saved as log files for later analysis. Any data that could be used to either identify the user of the web service or that contained sensitive contextual information, such as data showing the visited page or intention to seek help from the shelter, was extracted from the log files.

In evaluating the dark patterns in cookie consent banners, we used the definitions presented in the "Report of the work undertaken by the Cookie Banner Taskforce" by European Data Protection Board[3]. It outlines several specific scenarios that should be considered as dark patterns in cookie banners, of which we use four in this study: Absence of rejection button on the first layer of the cookie banner, pre-ticked selection boxes in regards to what cookies to consent to, deceptive button colors and deceptive button contrasts. In addition to these deceptive practices, we observed whether the analyzed website asked for consent for cookies at all. Privacy policies of the web services were inspected by reading them and corresponding information about data collection found in cookie banners, and then comparing them to the actual data collection that happened in these services. Specifically, we inspected whether these sources informed the user correctly of the data collection about the visited page, and whether this data leaked to third parties. The evaluation of dark patterns was conducted by two researchers, who compared their notes and debated about the differences, if any, in their findings until consensus was reached.

Since this study is about "personal data", we must take a moment to define it. For our purposes, the definition laid out in GDPR and the Finnish Office of the Data Protection Ombudsman is sufficient. That is, by the term "personal data", we refer to "all data related to an identified or identifiable person"[4]. By this definition, technical information such as IP addresses, device type, device identifying numbers, location data or any variable that identifies the user of the services counts as "personal data". It must also be noted that while all of these factors alone can not be used to identify someone, identification becomes possible when they are put together, and thus they fall under the definition of "personal data".

III. Results

Of the 22 studied shelter websites, 21 leaked some form of potentially identifying data (such as an IP address or a device identifier) to a third party. In all of these cases, the URL address of the current page was also sent to a third party, potentially disclosing the user's intent to seek help. Only one of the studied websites did not have any third-party analytics.

Figure 1 shows the numbers of third-party tools on the websites, each third party counted once per website. As can be seen, Google was present on 21 websites. Facebook and ShareThis receive sensitive data on 14 and 12 websites, respectively. In 50% of the studied cases, these same three actors were present on the website. Other recipients of leaked personal data were Wix, Matomo, Snoobi, LinkedIn and Socialstream, but unlike the "big three" actors, these were present only in a handful of cases.

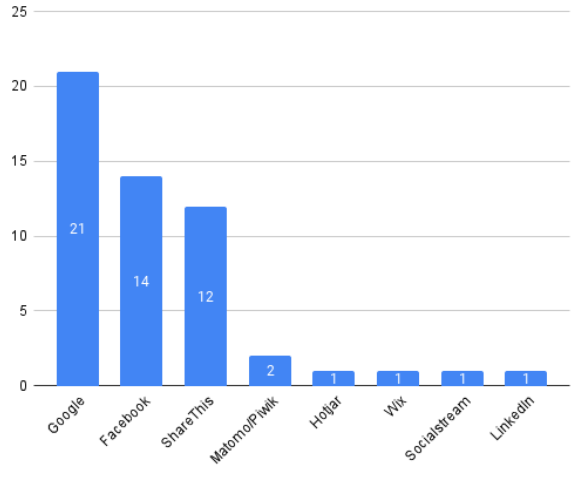

Fig. 1. Number of shelter websites using the third-party tools.

Several observations can be made based on the data we studied:

[3]https://edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en

[4]See https://gdpr.eu/eu-gdpr-personal-data/ and https://tietosuoja.fi/en/what-is-personal-data

1) *Nature of data*. In most of the cases, the leaked data could be used to, if not to definitely identify someone, at least be used in making an ”educated guess” as to the identity of the person using the shelters web service. Data such as this includes the IP address, cid number (client identification number, which is a device-browser pair specific identifier, allocated to every unique device-browser pair), device type, screen size and connection type, which especially combined together can be used to identify a specific user. This data, when accompanied by the current URL address, can cause serious data leaks when the context (seeking for help) is revealed to a third party.
2) *Role of Google*. Of all the data that was leaked, the data leaked to Google was the most sensitive in the sense that it usually contained elements most suited for identifying the user and the website user was currently viewing. Google was also the absolutely most common third party actor found in this study, being present on 21 out of 22 of the websites we analyzed and receiving sensitive personal data about page visits in 20 cases.
3) *The pattern of three*. On all 11 websites hosted under the domain of the Federation of Mother and Child Homes and Shelters, the three same third party actors (Google, Facebook/Meta and ShareThis) were present. On the other sites that were studied one, or in some cases two of these three might be present, but never all three at the same time. Mainly this indicates that this ”pattern of three” is a result of domain-wide policy adopted by the federation, regarding the analytics services used in the sites hosted at this one domain. This may indicate that the proprietors of the individual services are not even aware that this set of analytics services is deployed at the given site.

In total, Google Analytics was present in 95.5% of the 22 sampled websites. Facebook (59%) and ShareThis (54.5%) were present in slightly over half of the studied services, and a relative minority of sites had only Google (13.5%) or Google with another analytics service deployed (9%). Of the other analytics tools most common was Matomo, which was present on two of the inspected services (9%). One of these websites was the only service that did not use Google Analytics. Every other analytics service encountered in this study was deployed on only one service inspected (4.5%).

Matomo[5] is an open-source analytics service developed by a team of international developers for free. It has been recommended in previous studies regarding analytics services and privacy violations [11], [12], as in principle it allows the website proprietor to be in complete control of the data collected. In the case of the women’s shelters, however, it seems that both of the instances which use Matomo have acquired it from an external company offering services for actors in the Finnish public sector. As Matomo is deployed by the external actor, the principle of ”complete control over the data” seems to become compromised, at least in the sense that identifying data, such as the user’s IP address, is now leaked to a third party.

Most of the data leaked to third parties seemed to, as far as we could tell, end up in servers located outside of the Finnish borders. Three countries were the most prominent destinations: USA, Germany and Sweden. These three countries correlated strongly with the three most common analytics services used, in such a way that the data leaked to Google seemed to (usually) end up in USA, Facebook to Sweden and ShareThis to Germany, although also other services than Google sent the data to the servers located in the USA. In a handful of cases, the location of the servers could not be pinpointed with enough confidence. In one case the destination was quite likely Canada, and the data sent to Matomo and Snoobi seemed to stay within the Finnish borders, being stored in the servers of domestic hosting providers.

It has already been stated that the data leaked to Google Analytics was of the most incriminating kind; it contained cid, website URLs, screen size, device type and in some cases, even connection type. But how does this compare to the other analytics services inspected? Facebook seemed to collect a data profile roughly similar to Google, although perhaps slightly less privacy-violating (it did not contain the cid, for example); ShareThis, on the other hand, collected only the current website URL, session id and some data on the device used, such as the type of the operating system and the web browser. Other analytics services either collected data on a much smaller scope (Matomo, LinkedIn) or of a very different profile (Wix, Socialstream, Snoobi).

Shelter no. 20 was the only service to use Wix and Socialstream, and both of these tools collected a set of data quite different from that of the other tools. In addition to the current website URL, Wix seemed to collect only performance data, which results from this specific analytics service being bundled to the Wix in its capacity as a website publishing tool[6]. Socialstream, on the other hand, collected timezone, country and language information from the user of the website.

Snoobi and Hotjar were outliers among the analytics services inspected, but for quite different reasons. Snoobi was deployed on only one site (together with Google Analytics), and it seemed to collect only the country and the region where the shelter in question resides. Hotjar, on the other hand, did not seem to receive any kind of user data apart from the IP address and HTTP headers containing web browser and operating system information.

Only two websites, Shelters no. 8 and 22, were found to leak information regarding the user clicking elements with collapsible content. In both of these cases Facebook’s analytics service was the reason of the leak, and in one instance also Google Analytics. Information about the user opening collapsible info-boxes by clicking can give a third party more fine-grained information on the user’s confidential situation.

[5]https://matomo.org/

[6]https://www.wix.com/manage/analytics

All but one of the studied web services deployed at least one analytics service. The sole exception that did not have analytics of any kind was the Shelter no. 19. The only third party tool this service used was reCAPTCHA connected to Google servers, but apart from HTTP headers it did not leak any sensitive personal data. The only service that had analytics but did not deploy Google Analytics was the Shelter no. 12, which used only the Matomo analytics service.

Unfortunately, the sensitive information about the current website URL was leaked by every website that used any analytics at all, although it must be noted that not all analytics services leaked this information. The exact numbers are shown in Figure 2. As can be observed, they correlate strongly with the presence of the analytics in the first place. Google is the most frequent collector of the current URL address (20 occurrences), followed by Facebook (14) and ShareThis (12). However, notably Socialstream, Snoobi and Hotjar did not leak this data.

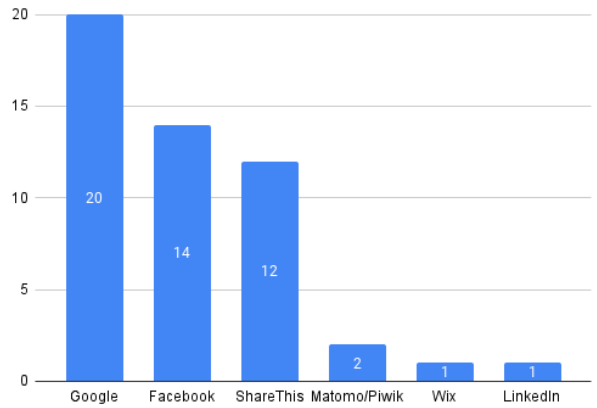

Fig. 2. The occurrences of third-party tools leaking the current URL address.

The results of privacy policy analysis can be seen in the Table I. The table also shows whether the studied websites asked for consent. The privacy policies of the 11 shelters which were hosted on the domain of the Federation of Mother and Child Homes and Shelters were identical, and failed to adequately inform the user of the data collected. Specifically, the privacy policy presented was vaguely worded and very short, not indicating clearly enough that identifying personal data, such as IP addresses, or sensitive contextual data, such as the current website URL, is being collected. Of the remaining 11 shelters, only six had a privacy policy, and of these only four informed the user transparently. Curiously, this lack of privacy policy documents did not exactly correlate with the lack of the cookie consent banners, which were absent from five websites. Instead, both Shelters no. 13 and no. 15 had privacy policies, but no observable means to give consent to cookies, while Shelters no. 21 and 22 did not have policy, but had the consent banner in place. The situation is made worse by the fact that several of these, for example the aforementioned Shelter no. 15, claim in their privacy policy to not to collect identifying information on their users, then lack the means of not consenting to the data collection and then just collect the data anyway. On the other hand, most of the websites which had privacy policies and the option to consent to cookies presented the nature of data they collected very vaguely, as discussed previously.

TABLE I
DISCREPANCIES BETWEEN THE STUDIED PRIVACY POLICY DOCUMENTS AND ACTUAL DATA PROCESSING.

Website	Website asks for consent	Privacy policy exists	Admits collecting personal data	Data is collected in accordance with the policy
Shelter no. 1				
Shelter no. 2				
Shelter no. 3				
Shelter no. 4				
Shelter no. 5				
Shelter no. 6				
Shelter no. 7				
Shelter no. 8				
Shelter no. 9				
Shelter no. 10				
Shelter no. 11				
Shelter no. 12				
Shelter no. 13				
Shelter no. 14				
Shelter no. 15				
Shelter no. 16				
Shelter no. 17				
Shelter no. 18				
Shelter no. 19				
Shelter no. 20				
Shelter no. 21				
Shelter no. 22				

The dark patterns found on cookie banners of the analyzed women's shelter websites are shown in Table II. The green color implies a positive result, while red indicates that the website has failed to follow a recommended practice. Five websites had no cookie banners and failed to ask for consent. Therefore, the user has no easy way to turn off cookies or decline analytics services upon arrival at the websites. The dark patterns of these five websites could not be further analyzed, which is why they are marked in black.

It should be noted that the failure to inform the user about the cookies used to collect data on the site is a direct breach of the GDPR, is essentially illegal and may result in legal consequences[7]. This behavior was exhibited by two of the studied websites, which had neither privacy policy documents nor cookie consent banners.

Of the remaining 17 websites which had cookie banners, one website (Shelter no. 12) did not display a reject button on the first layer of the cookie banner. This number can be considered a relatively good result. On the website with the dark pattern, however, the process of turning off cookies thus becomes more difficult for the user, who may be in a

[7]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

TABLE II
DARK PATTERNS ON COOKIE BANNERS OF WOMEN'S SHELTER WEBSITES.

Website	Type A Absence of rejection button	Type B Pre-ticked consent boxes	Type D Deceptive colors	Type E Deceptive contrast
Shelter no. 1				
Shelter no. 2				
Shelter no. 3				
Shelter no. 4				
Shelter no. 5				
Shelter no. 6				
Shelter no. 7				
Shelter no. 8				
Shelter no. 9				
Shelter no. 10				
Shelter no. 11				
Shelter no. 12				
Shelter no. 13				
Shelter no. 14				
Shelter no. 15				
Shelter no. 16				
Shelter no. 17				
Shelter no. 18				
Shelter no. 19				
Shelter no. 20				
Shelter no. 21				
Shelter no. 22				

hurry and distressed when arriving at the website. Furthermore, on one occasion, there were pre-ticked boxes on the studied cookie banners. Deceiving the user into giving consent without clear and affirmative user action like this violates the GDPR. Recital 32 of the GDPR states that silence, pre-ticked boxes or inactivity should not constitute consent.[8] Lastly, the most frequent design flaw, present in all 17 banners, is the use of deceptive colors and contrast (see e.g. [13]). The accept button is made to stand out from the background and from the reject button so clearly that a user, in an anxious state of mind, can easily choose the accept option. It is very questionable, however, whether this can be called an informed decision.

IV. DISCUSSION

Women's shelter websites can be considered essential services that should take users' privacy very seriously and strive to remain free of any third-party services that may track visitors. Nevertheless, our results show that these websites may jeopardize user privacy when all cookies are consented to. Against this background, it is questionable that they use any tools for analyzing user behavior and traffic at all, as it is justifiable to ask what added value do these tools bring to the web services of this nature. People seeking information about women's shelters or domestic violence are usually doing so in situations that are dire [14], and for motivations that are quite straight-forward, and it is hard to see how exactly the analytics tools studied here could help to improve these services.

[8]https://www.privacy-regulation.eu/en/recital-32-GDPR.htm

However, it should be considered that the ubiquitousness of the analytics services deployed at these sites might simply be a result of "ignorance on the buyer's part". In other words, it is quite probable that the websites have been commissioned from outside developers, who are always more than happy to sell all kinds of additional features to their products, regardless of whether the customers are aware of whether they need them or not. This creates a situation where the people making the decision on what to buy might be unsure of what they actually need, and in this fugue state the analytics services are added to the package "just because that is the standard nowadays", without actual forethought on their usefulness or their potential downsides.

Other explanation, applicable on exactly 50% of the studied cases is the fact that half of the studied sites are hosted on the same domain. All of these sites use exactly the same set of analytics tools, namely Google, Facebook and ShareThis. It is not far-fetched to make an induction that the proprietors of these sites have not made individual decisions about using the analytics services they are working with, but have rather had this decision thrust upon them by either the proprietor of the domain they are using, or by some package deal from the company that has developed all of these websites. Again, the issues of using analytics just because it is a standard practice and not fully appreciating the consequences may apply here too.

According to our results, the most common contextual piece of personal data to be leaked was the URL of the current page. While this is not a privacy-violating piece of data by itself, it becomes very sensitive when combined with identifying details, and is a very central part of the problematic data leaks observed here. It is notable that while all websites that used analytics did leak this piece of data, not all of the tools used did so. If the shelter website has to use analytics services, the least they could do is choosing the tools that do not leak this information, or alternatively, reconfiguring the leaky tools.

Leaking personal data related to using shelter websites can potentially have severe consequences. Third-party services frequently utilize tracking technologies, recording user behavior across several websites. Consequently, detailed profiles revealing sensitive information about violence victims can be created. When a website visitor's personal data is shared with third-party services, it could also potentially lead to discriminatory practices, stigmatization or re-victimization, as the visitor's personal history and potential association with violence can leak to unintended parties (cf. [15]). Moreover, discovering that their personal data has leaked to third parties may erode trust and confidence that victims have in shelters and support systems in general.

In terms of software engineering and web development, there are multiple issues the maintainers of the studied websites should take into account. We recommend the following measures to improve the privacy and confidentiality of women's shelter websites:

- *Perform an analysis of outgoing network traffic*. A thorough network traffic analysis can be performed in a

manner similar to this study. In sensitive online services like women's shelter websites, it is essential to ensure that the user's personal data does not leak to third parties such as technology giants like Google. Arguably, data leaks should be prevented even if the user ostensibly consents to cookies and analytics services. Although users may click the accept button upon arriving to the website, they may not be in the right state of mind to assess the risks of third-party services or understand that information on their identity, visited pages, and help-seeking behavior may leak.

- *Remove third-party services*. Based on the results of network traffic analysis, third-party services should be removed. It is difficult to justify their use in a sensitive context such as women's shelter websites. If web analytics are deemed absolutely necessary, local analytics solutions should be used [11]. These analytics tools are implemented so that the organization itself controls the collected data and users' personal data is not leaked to third parties.
- *Carefully review cookie banners and remove dark patterns*. It is problematic that there are many ready-made cookie banner solutions which supposedly help the websites achieve GDPR compliance, but ironically also contain dark patterns that do not align with the principles of the GDPR. Therefore, web developers must take special care either not to choose such cookie consent management platforms, or to modify them to omit any deceptive practices.

V. Conclusions

In this study, we have comprehensively demonstrated that almost all (95.5%) of the surveyed Finnish women's shelters leak personal data about their users to third parties. This happens through third-party tools deployed at the shelters' websites, and it is to a degree enabled by misleading, or otherwise faulty, cookie consent banners and erroneously presented privacy policies which are at odds with the GDPR.

Our study showed how identifying personal data is leaked to third parties. While many of the leaked data items observed in this study could not be used alone to identify a specific user accurately, these individual items can also be combined to track individual users. Especially technology giants such as Google and Meta are very likely to have the capability to create an accurate profile of the website user. This goes to show that while the given privacy policy may claim that the site is not collecting any identifiable information, thus leading to user giving their consent to data collection, this might be true de jure, but not de facto.

There is a clear and urgent need to improve the privacy of women's shelter websites so that they do not leak identifying information accompanied by sensitive contextual information such as the fact that the visitor is seeking help. Removing unjustified third-party services, auditing the data leaks on the websites as well as GDPR-compliant cookie banners and privacy policies are crucial measures to achieve this. We hope that this research serves as a catalyst for change by shedding light on privacy challenges within women's shelter websites. It is worth noting that women's shelters are only one example of essential services where these kinds of critical data leaks of sensitive nature occur. In this sense, our research also contributes to the broader discourse on online privacy and security, inspiring the implementation of enhanced measures to safeguard sensitive personal data. Our future work involves privacy of other essential websites such as mental health services and medical center websites.

References

[1] M. E. Bagwell-Gray and E. Bartholmey, "Safety and services for survivors of intimate partner violence: A researcher–practitioner dialogue on the impact of covid-19." *Psychological Trauma: Theory, Research, Practice, and Policy*, vol. 12, no. S1, p. S205, 2020.

[2] L. H. Madsen, L. V. Blitz, D. McCorkle, and P. G. Panzer, "Sanctuary in a domestic violence shelter: A team approach to healing," *Psychiatric Quarterly*, vol. 74, pp. 155–171, 2003.

[3] K. E. Ravi, A. Rai, and R. V. Schrag, "Survivors' experiences of intimate partner violence and shelter utilization during covid-19," *Journal of family violence*, vol. 37, no. 6, pp. 979–990, 2022.

[4] E. Freer, "Are resources out of reach? analyzing the accessibility of domestic violence shelter services," *Social Science Quarterly*, vol. 103, no. 3, pp. 550–564, 2022.

[5] S. A. Chanley, J. J. Chanley Jr, and H. E. Campbell, "Providing refuge: the value of domestic violence shelter services," *The American Review of Public Administration*, vol. 31, no. 4, pp. 393–413, 2001.

[6] R. Constantino, Y. Kim, and P. A. Crane, "Effects of a social support intervention on health outcomes in residents of a domestic violence shelter: A pilot study," *Issues in mental health nursing*, vol. 26, no. 6, pp. 575–590, 2005.

[7] C. N. Wathen and H. L. MacMillan, "Interventions for violence against women: scientific review," *Jama*, vol. 289, no. 5, pp. 589–600, 2003.

[8] A. L. Few, "The voices of black and white rural battered women in domestic violence shelters," *Family Relations*, vol. 54, no. 4, pp. 488–500, 2005.

[9] R. Campbell, C. M. Sullivan, and W. S. Davidson, "Women who use domestic violence shelters changes in depression over time," *Psychology of Women Quarterly*, vol. 19, no. 2, pp. 237–255, 1995.

[10] K. J. Ferraro, "Negotiating trouble in a battered women's shelter," *Urban Life*, vol. 12, no. 3, pp. 287–306, 1983.

[11] J. Gamalielsson, B. Lundell, S. Butler, C. Brax, T. Persson, A. Mattsson, T. Gustavsson, J. Feist, and E. Lönroth, "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.

[12] T. Heino, R. Carlsson, S. Rauti, and V. Leppänen, "Assessing discrepancies between network traffic and privacy policies of public sector web services," in *ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security*, 2022, pp. 1–6.

[13] C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, "Dark patterns and the legal requirements of consent banners: An interaction criticism perspective," *CoRR*, vol. abs/2009.10194, 2020. [Online]. Available: https://arxiv.org/abs/2009.10194

[14] Y. M. Luna, *An analysis of how battered women in a rural community shelter are served by welfare*. Arizona State University, 1997.

[15] C. Chen, N. Dell, and F. Roesner, "Computer security and privacy in the interactions between victim service providers and human trafficking survivors," in *USENIX Security Symposium*, 2019, pp. 89–104.