Third-Party Data Leaks and Dark Patterns in Finnish Political Websites

Panu Puhtila
University of Turku
Department of Computing
Turku, Finland

Timi Heino
University of Turku
Department of Computing
Turku, Finland

Sampsa Rauti
University of Turku
Department of Computing
Turku, Finland

ABSTRACT

In the modern digital age, political parties extensively use websites as platforms for communication, engagement, and fundraising. It is important to ensure that personal data is safe when visiting these websites. For example, if pages visited by the user or search terms they used leak to third parties, this data, connected to identifying information such as IP addresses, may give clues about political affiliation. In this paper, we conduct a survey on the data leaks to third parties happening in Finnish political websites. In total, we surveyed 26 websites (main website, party chairperson's website, and e-shop/donation website of each party), and our results indicate that 19 of the 26 analyzed websites leak potentially sensitive personal data to third parties, most often to Google and Meta. Furthermore, there were leaks of personal data on all surveyed party websites, implying data leaks happen across the entire political spectrum. There is an urgent need for better data protection measures on political websites. The implications of political opinions potentially leaking to third parties can be serious, jeopardizing individuals' autonomy and democratic rights.

KEYWORDS

Political party, online privacy, data leaks, user tracking, web analytics

ACM Reference Format:
Panu Puhtila, Timi Heino, and Sampsa Rauti. 2024. Third-Party Data Leaks and Dark Patterns in Finnish Political Websites. In *International Conference on Computer Systems and Technologies 2024 (CompSysTech '24), June 14–15, 2024, Ruse, Bulgaria.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3674912.3675248

1 INTRODUCTION

During the past decade, information and communications technology has reached an ubiquitous status in society, fundamentally transforming our everyday experience. Together with this rise of the technology have developed new avenues for its use; on the other hand, the information it can provide for its users, and on the other the data that can be extracted from their interactions in the digital realm. The latter – the data on users' behavior online, what links they click and what pages they visit – is the new oil, an electric stream of revenue that can be extracted and sold for profit. For this reason, a whole industry has developed around this venture, an industry where sensitive pieces of data like our political opinions can become commodities to be sold, bought, and used to profile us.

Third-party web analytics are an usual way for technological giants to collect personal data on users. These services, such as Google Analytics, are very popular on modern websites today. This is also true for the websites of political parties. Since the political parties are central actors of society, being responsible for the organization and running of the parliament and the government, their actions should be held to a higher degree of accountability than most of the other societal institutions. Not only should the citizenry be able to trust that at least these actors do not act in illegal or morally dubious ways, but that the privacy of their personal political beliefs is not jeopardized. After all, privacy of political opinions is one of the foundations upon which our form of representative democracy is built upon, and eroding trust in this institution could have severe consequences for the society at large. Under the GDPR, political opinions are considered a special category of personal data that requires strict protection. Thus, we feel that there is a pressing need to study how the visitor data is handled by the political parties, and whether the users of their websites can be certain that this data is not used for potentially malicious ends, such as political profiling.

In this paper, we investigate the websites of the political parties operating in Finland, to determine whether they leak the personal data to third party actors and whether they use dark patterns in their cookie consent banner designs. In total, there are 17 registered political parties in Finland, but only 9 of these are popular enough to have representatives in the parliament. For this reason, we have chosen to focus on these 9, and exclude the smaller parties from this investigation, as their societal influence is much smaller.

The rest of the paper is organized as follows. In Section 2, we take a brief overview on the related research papers. In Section 3, we explain our research methodology and study setting extensively. In Section 4, our results are represented. In Section 5, we discuss the implications of our results. Finally, in Section 6, we provide the definite conclusions that can be drawn from this study.

2 RELATED WORK

The specific subject of the current study – whether the personal data leaks from the websites of political parties – has not received prior attention from scholars. However, studies have been conducted on the subject of political parties and political media websites and their relation to matters of privacy. As these studies are at least tangentially related to our work, we will take an overview of them here. Another aspect of interest in the current study is the use of dark patterns, we also take a look at the research done on this

CompSysTech '24, June 14–15, 2024, Ruse, Bulgaria

ACM ISBN 979-8-4007-1684-3/24/06
https://doi.org/10.1145/3674912.3675248

phenomenon. These two topics have been separated into their respective subsections for the sake of clarity.

2.1 Studies on political websites and data collection

Already in 2009, Howard and Kreiss [11] conducted a large-scale study in which they investigated how political parties in the major countries of the anglosphere, i.e. USA, United Kingdom, Australia and Canada, handled the personal information of their supporters which had ended up in the parties keeping, and what kind of legislation these parties created to govern these kinds of transactions. Their findings were quite varied, with one reason behind this being differences in legislation between these four countries. In Australia, for example, political parties were at this time specifically exempt from obeying privacy laws and regulations, and as a consequence many politicians were involved in data-mining business where they callously used the information gained from their supporters for monetary gain.

Agarwal et al. [1] published a paper in 2021, where they studied 103 politically motivated Indian media websites, each of which they categorized to either be predominantly in the left, right or centre. Agarval et al. studied whether these websites used analytical tools and tracking cookies, and whether this somehow correlated with their political bias. Their results indicated that there were strong correlations between the professed political stance of the media website and the method of data collection mostly used, for example that those websites oriented to the political centre were more prone to use invisible tracking pixel -based solutions, while leftist media used more tracking cookies.

Richards and Ozok [20] studied the relation between the design of the political campaign websites, privacy policy documents and the perceived trust towards the candidates for political positions in their 2018 paper. One of their research questions was "*Do political website visitors believe that they can trust the candidate more if the website has a clearly written privacy policy when compared to campaign websites which do not?*". Their results indicated, with 54% of the informants saying that this increases trust in the candidate and 69% saying that reading the privacy policy is important but at the same time 49% saying that they never read the privacy policy and 37% saying that they only rarely read it, that people are prone to think one way and act another.

Samarasinghe et al. [21] conducted a survey on the privacy violations in the government websites and Android applications. Their study encompassed 150244 government affiliated websites and 1066 government apps, from every country on the globe. They concluded that the majority of both the websites and apps leaked personal data to third parties, most prominently to Google Analytics.

Kirkizh et al. [18] conducted a study in which they analyzed the data collected from 19 million page visits by 1003 test participants, to determine how well the website users can be politically profiled just from the arbitrary choices they make in non-politically motivated websites. Their findings suggest that the potentials for this kind of profiling are quite limited in scope.

Bennett has published several articles [2, 3], in which he has studied the developments of "data driven campaigning", in other words the use of political profiling of voters by the political parties in targeting and designing political campaign advertisements, or what is known as microtargeting. He has concluded that while thus far the countries of the anglosphere are more prominent in the use of this kind of campaign techniques compared to European countries, these practices would most likely become more common in European politics as well.

2.2 Studies on dark patterns

Bosch et al. were among the first to publish on dark patterns [8]. They, among other things, pioneered the classification of this phenomena. Gray et al. [10] studied dark patterns in UX design and concluded that the corporate greed was a great motivator for these practices. Cara studied in her paper [9] dark patterns, reaching similar results as Gray et al.[10] Mathur et al. [15] conducted a large-scale survey with automated web crawlers across roughly 11 000 websites, in which they encountered 1818 different dark patterns in use. Waldman [23] conducted research on how dark patterns are used to manipulate consent to data collection using cognitive biases. Nouwens et al. studied [19] the five biggest consent management platforms (CMP) in the 10 000 most popular British websites, and how well they complied with the GDPR. As a part of the research they tested the effects of dark patterns on the users. Their results indicated, for example, that the absence of the "decline" button on the first layer of the consent management banner increased the granting of consent to cookies by as much as 22–23%. Narayanan et al. [17] studied the intentional design and usage of dark patterns by web companies for financial profit. Their paper raised concerns for the regulatory backslash and reputational damage to the industry for such practices. Bhoot et al.[14] wrote a paper where they explored the questions of what makes people susceptible to dark patterns.

Mathur et al. [16] researched the factors that define the dark patterns, and proposed solutions to more empirical ways to categorize them. Krisam et al. [13] examined the dark patterns in the top 500 German websites. Among their findings was that at least 85% of the websites use visual distractions to manipulate the user to consent to data collection, and only 21.5% gave the user a direct choice of abstaining from data collection. Bongard-Blanchy et al.[6] conducted a large-scale interview study, where they discovered that the users usually are both aware of being affected by the dark patterns, and feel powerless to do anything for this. This effect was more pronounced with younger informants.

Kocyigit et al. [12] did a structural study on cookie banners, specifically on how their multiple layer layouts relate to the use of dark patterns. Borberg et al. [7] researched the psychological dimension of dark patterns and how it affected users' decision making, and concluded that they have a significant effect on the user experience of the consent banner, up to the point of even affecting whether the user remembered giving consent in the first place. Berens et al. [4, 5] examined the cookie consent banners. Their results showed that especially dark patterns that worked on visual mechanisms and the contents of the texts in the accept and decline -buttons directly influenced the decision to consent to cookies.

3 METHODOLOGY AND STUDY SETTING

The target of the current study are the websites of those political parties which operated in Finland and had at least one representative in the Finnish Parliament at the time of the start and end of the investigation. That is to say, these are established parties with more-or-less consistent large voter bases, that are powerful enough to have significant impact in the national politics of Finland, as opposed to minor parties which have only marginal support and thus no substantial impact in the political landscape. There were 10 such parties, of which one has since then dropped out of the parliament due to not getting enough votes in the 2023 parliamentary elections. For this reason, this one party which is no longer present in the parliament was excluded from the results of the current study.

In addition to the main websites of the parties, we also investigated their current party chairperson's personal website, and websites through which people can donate money to the party or, if the party did not have a site for donation, online marketplaces, if such pages existed. All of the studied parties had a main website, and all of them also had a personal website for the party chairperson. 5 parties had an online marketplace, through which support merchandise was sold, and 3 had a donation website. Thus, the total number of studied websites, when all categories are summed up, was 26. However, to ensure the anonymity of the party which did not have e-shop nor donation website we have treated it as having them, and thus for this reason Table 1, which details the results of the investigation into dark patterns, includes a row presenting this non-existent e-shop as if it had existed.

Websites of the political parties were studied in the following way. All tests were conducted with the Google Chrome browser. Upon arrival to the landing page of the website, the researcher opened the Google Chrome Developer Tools, and disabled caches to prevent any previously cached information from interfering with the test results. Developer tools were set to record all network traffic. After this the website was reloaded. All cookie consent banners and privacy policy documents were saved either in screenshots, PDF files or HTML files. After this, full consent to all cookies, marketing and other analytics -related actions was given.

After this the researcher navigated to the "News" subpage, or similar, after which they navigated to the "Joining the party" -subpage. If there was a form through which to join the party, it was filled, but not sent. If the "Joining the party" opened up into a new browser tab, this new site was also studied with a similar process. After this the researcher navigated to the "Search" functionality or subpage, entered the search phrase "Poliittinen ohjelma" (Political program in English) and clicked the first result.

The recordings logged by the Google Chrome Developer Tools during this procedure were saved in .HAR files, which were later analyzed to determine what kind of traffic happened during the navigation. In this research, we specifically focused on the leaks of three different data objects which were:

(1) *Visited page URL:* The page URL implies the user is visiting the party-affiliated websites and thus has a potential political interest towards the party.
(2) *Clicking of a button:* This refers to "Make donation" and "Add to shopping cart" buttons found in the party e-shops and donation websites. The information about clicking these buttons may indicate that the website user supports the party in question.
(3) *Search term:* The leaked search term (e.g. when the search is used to look for the political agenda of the party) can often indicate in-depth interest in the party ideology, which may imply support for the party in question.

In addition to the data leaks, we also conducted a survey on whether dark patterns were used in the cookie consent banners of the party-affiliated websites. In this work, we used the definitions of the European Data Protection Boards Cookie Consent Banner Taskforce, which has laid them out in their "Report of the work undertaken"[1]. This document details many dark patterns, of which we focused on four specific ones as these four are the most unambiguous to measure, which are:

- *Absence of the "reject cookies" button on the first layer of the cookie banner*. This category of dark patterns specifically means that the ability to refuse the data collection is not situated on the immediate first layer of the cookie consent banner, and is thus hidden to mislead the user.
- *Pre-ticked consent boxes*. These are interactive elements that are meant to be used for specifying which cookies to consent to, which are set by default to allow data collection. Having such elements pre-ticked is insufficient for obtaining unambiguous and freely given consent.
- *Deceptive use of colors*. Psychological manipulation of the user by the deployment of specific colors. Example of this would be the intentional use of a certain color due to its known psychological effects [17].
- *Deceptive use of contrasts*. This category is similar to the previous one, but is more concerned with how the colors are used together rather than individual colors.

Since this paper is concerned with leaks of personal data, the concept of such data must be defined. Here we will adhere to the one given in GDPR of the European Union and also used by the Finnish Office of the Data Protection Ombudsman[2]. By this definition, personal data is "all data related to an identified or identifiable person". In practice, this means technical information such as device identifiers, IP addresses, accurate location data or any other data point that can be used to identify the user of the website. It should be understood that while technical details such as device type or screen resolution can not directly be used to identify the user, when put together these data items can be used in digital fingerprinting, or at least in making very educated guesses about the identity of a specific person. For this reason, they fall under the purview of personal data.

4 RESULTS

4.1 Data leaks

First, it must be noted that the difference in the use of web analytics tools between parties was not very great. None of the parties passed with flying colors, as all of them had at least one data leak in some of their affiliated websites. All of the parties used between

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

Table 1: Dark patterns on the cookie banners of the Finnish political websites.

Website	Asks for consent	Absence of reject button	Pre-ticked consent boxes	Deceptive colors	Deceptive contrasts
Party nr. 1 website					
Party nr. 1 e-shop					
Party nr. 1 chairperson's website					
Party nr. 2 website					
Party nr. 2 e-shop					
Party nr. 2 chairperson's website					
Party nr. 3 website					
Party nr. 3 e-shop					
Party nr. 3 chairperson's website					
Party nr. 4 website					
Party nr. 4 e-shop					
Party nr. 4 chairperson's website					
Party nr. 5 website					
Party nr. 5 e-shop					
Party nr. 5 chairperson's website					
Party nr. 6 website					
Party nr. 6 e-shop					
Party nr. 6 chairperson's website					
Party nr. 7 website					
Party nr. 7 e-shop					
Party nr. 7 chairperson's website					
Party nr. 8 website					
Party nr. 8 e-shop					
Party nr. 8 chairperson's website					
Party nr. 9 website					
Party nr. 9 e-shop					
Party nr. 9 chairperson's website					

1 to 3 web analytics tools in their websites, with the averages being 1.35 per website and 2.33 per party. The absolutely most common analytics tool encountered was Google Analytics, which apart from one exception was found from every website which used analytics. Considering that Google Analytics is the most common web analytics tool globally, this is hardly a surprising result.

In total 19/26 of the studied websites leaked data to third parties. Breaking down the results into categories, we can see from Figure 1 that

- 8/9 of the main party websites leaked personal data to at least one source.
- 6/8 of the party e-shops or donation platforms leaked personal data to at least one source.
- 5/9 of the party chairpersons' websites leaked personal data to at least one source.

Looking at the data leak categories, 19/26 (73.1%) of the websites leaked the website URL to at least one third party. That is to say, every page that had data leaks leaked this data item. Google Analytics was the main, but not the only, reason for the data leaks in this category. 6/8 (75%) of online marketplaces or donation websites leaked the information about clicking the button for making donations or adding a support merchandise to the shopping cart. In all of these instances, the information was leaked to Google Analytics. Total of 9/26 (34.6%) websites in this survey leaked the search term to at least one third party. Most often this was leaked to Google, but other third parties observed were Giosg and Facebook.

It should be understood that the majority of the surveyed websites leaked data to more than one third-party recipient. Thus, while the number of websites was 26, the total number of leakages was 35, between 9 political parties and 8 analytics services. The most common recipient of these leaks was Google Analytics, but Facebook (Meta Pixel), Adform, Twitter, Giosg, Readpeak, Typekit and Cavai were also responsible for these leaks. As can be seen in Figure 1, Google Analytics and Meta Pixel dominated the leakages clearly, with 17/35 (48.6%) of the leakages happening due to Google Analytics, and 10/35 (28.6%) due to Meta Pixel. All of the remaining four analytics services received only one leak each. As each of the leaks correlates with a party, this means that 8/9 of the parties in the Finnish Parliament leaked data to Google Analytics, and 6 to Meta Pixel. One of the parties leaked data only to Twitter. Considering

the potentially sensitive political nature of the leaked data, these numbers are nothing short of appalling.

While the parties leaked personal data 35 times, the total number of leaked data items was 32 which can be seen in Figure 2. The difference between the total numbers of Figure 1 and Figure 2 is justified by the calculation methods. No matter how many times a website leaked data to a certain analytics service, the existence of that service is calculated only once (Figure 1), but if a website leaked several data items to same analytics service, those occurrences were all included in the total number (Figure 2). For example, Party 9 eShop leaked 3 data items to Google Analytics, and thus total number of leaked data items was incremented by 3 and the number of leakages to Google Analytics was incremented by 1. When we consider the types of data leaked, it can be seen in Figure 2 that the most common data leak type was the visited page URL, which constituted 19/32 (59.4%) of the leaks. The second largest leak type was the search term, which had the share of 9/32 (28.1%). The third category, clicking of the button, amounted to the remaining 4/32 (12.5%) of the leaks.

The party with the fewest leaks among all was party number 4, which exhibited only one data leak. This leak happened at their party chairperson's website, was a URL leak, and was received by Twitter. Otherwise, all of the other parties had multiple points of leakage across their affiliated websites, with 3.89 data leaks per party being the average.

There does not seem to be a correlation between the use of web analytics, the subsequent leakage of personal data and the political stances of the party. Parties across the political spectrum from left to right and centre fared equally poorly in this survey, and with the exception of the one party that only leaked one data item to Twitter there were no big differences between the parties. Finally, it is important to keep in mind that while the URLs and search terms, for example, are not by themselves sensitive data, the data leaks become very problematic when this information is combined with IP addresses or other technical data items that can be used to uniquely identify the user either alone or when combined together. Moreover, the major analytics services like Google and Meta can track users' activities on various websites and connect them to specific user accounts. This often makes it possible to associate users' real names with specific page visits or searches.

4.2 Dark patterns

The results from our investigation of the dark patterns in these websites can be seen in Table 1. In the table, the red color describes a negative outcome (the website does not ask for consent or a dark pattern is present). The blue color means a positive outcome (the website asks for consent or a dark pattern is absent). A black row indicates that the studied website did not have a cookie consent banner.

The most common forms of dark patterns encountered were the use of deceptive contrasts and colors, which were present in 9/26 (34.6%) of the websites. 6/26 (23.1%) of the inspected websites had the rejection button hidden from the first layer of the cookie consent banner, and only one (3.8%) used the pre-ticked consent boxes. The latter result can be seen as positively small, as while the use of dark patterns in general is usually only morally questionable, not outright illegal, the use of the pre-ticked consent boxes is understood as per the GDPR to not be a valid form of giving consent to data collection and can thus be considered illegal.

Apart from these, two other notable phenomena were detected, which are not directly classified as dark patterns, but are related to them and are thus presented under this subsection. First off, a large proportion of the inspected websites, precisely 10/26 (38.5%) did not have cookie consent banners at all, although some of these websites used web analytics tools and collected user information. These are marked in Table 1 as completely black rows. Second, there were 2/26 (7.7%) websites, both belonging to the same party which lacked the ability to reject consent to cookies altogether. Both of the situations encountered are direct breaches of the GDPR, and it is quite alarming that they were encountered at all, and on top of that, in such a high quantity.

5 DISCUSSION

The key takeaways from our results are the following:

- **Role of Google Analytics & Facebook:** These two analytics services accounted for the majority of the data leaks, together comprising 27/35 (77.1%) of all leaks. This is not surprising, as they are both two of the largest website analytics platforms globally[3][4], but also have been shown in previous studies to usually be the main reason for data leaks in websites.[22]
- **Page URL leaks:** This data item was the most common point of interest to leak, and was observed to do so in 19/26 (73.1%) of the studied websites.
- **No great differences between parties:** Apart from one party, which did not use any kinds of analytics tools in their website, all of the others had quite similar numbers of analytics deployed, with the average being 1.35 analytics tools per party website and 2.33 per party.
- **Complete absence of cookie consent banners:** In this study, we observed a particularly high proportion of complete absence of cookie consent banners. This situation was witnessed in 10/26 (38.5%) of the websites, and merits certain consideration.

The results obtained in this research are alarming. The stark majority of the studied party websites leaked personal data to third parties, which would not only be unacceptable from moral perspective, but can be also be problematic in the light of the GDPR, especially as the leaked data may contain political opinions and may end up in servers situated outside the borders of the European Union in some cases. This is of course ironic, as the parties themselves have participated in formulating this regulation as part of the European Parliament. What is more, the users, even though they would consent to data collection in general, may not understand and be properly informed of the fact that sensitive personal data concerning their political opinions may be collected.

This is also a matter of social trust. If the constituents can not have faith in the political parties to act according to the rule of law these parties themselves have had a hand in enacting, the repercussions for the society at large can be wide-ranging and

[3]https://w3techs.com/technologies/details/ta-googleanalytics
[4]https://techhq.com/2023/07/why-is-the-meta-pixel-at-heart-of-data-privacy-cases/

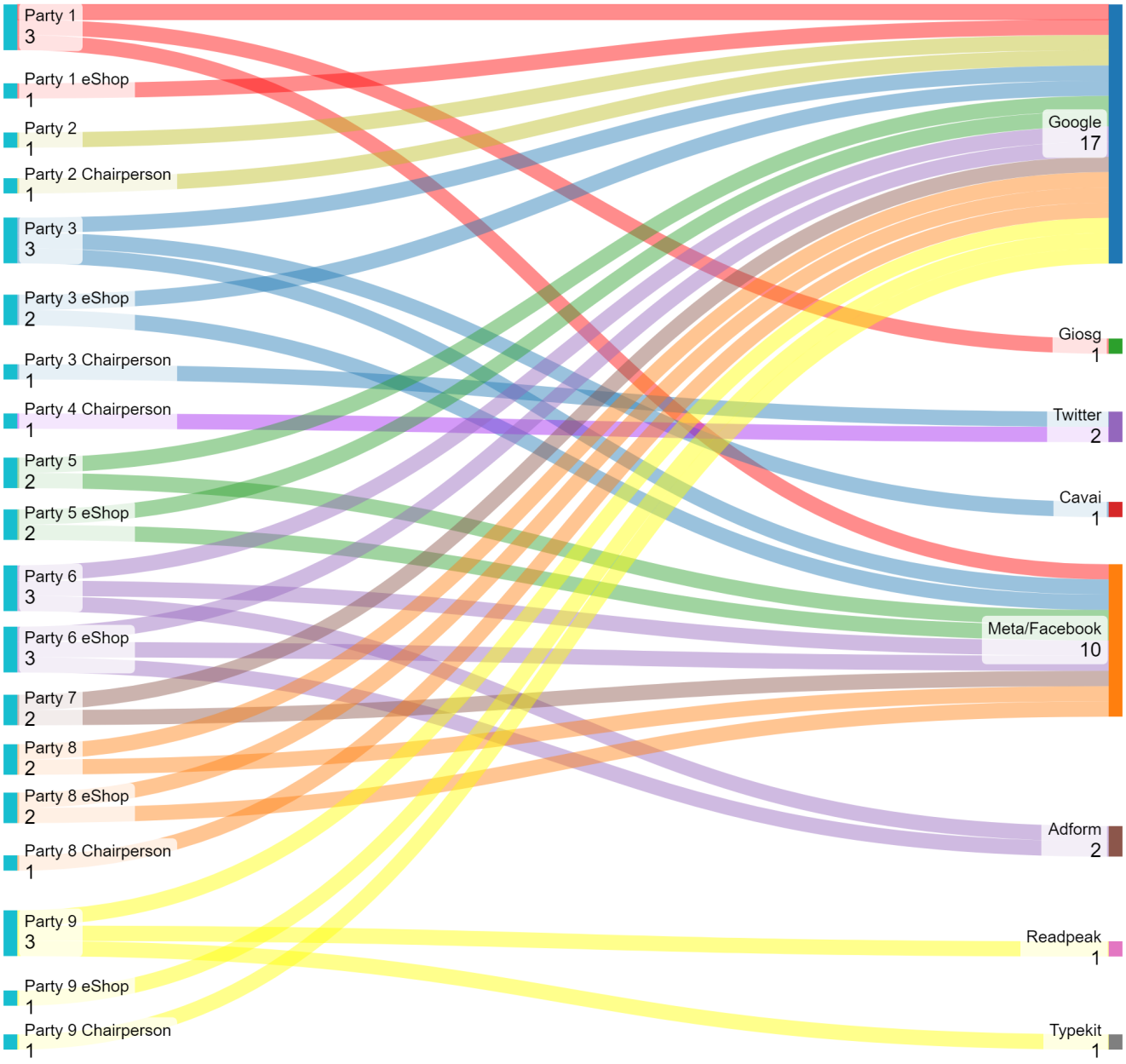

Figure 1: Number of data leaks and third parties who received leaked data.

devastating. The situation is made even worse if these constituents themselves are the victims of such activities.

The privacy of political opinions is a very sensitive issue in democratic societies, to such a degree that it is often enshrined in law, such as is the case in Finland. If websites directly affiliated with political parties leak data concerning their users' political opinions along with the data that can be used to identify these users, moral concerns are raised.

Against this context it is disheartening to see that the absolute majority, 8 out of 9 parties, used web analytics that transfer potentially sensitive personal data to third parties, and thus contributed towards the breach of this implied societal trust. This finding implies that the maintainers of party websites do not pay sufficient attention to the privacy of their websites. While it is likely data leaks are caused inadvertently, organizations that operate on large budgets should be able to do better. Political parties that compete for the highest political power in Finland should help prevent this

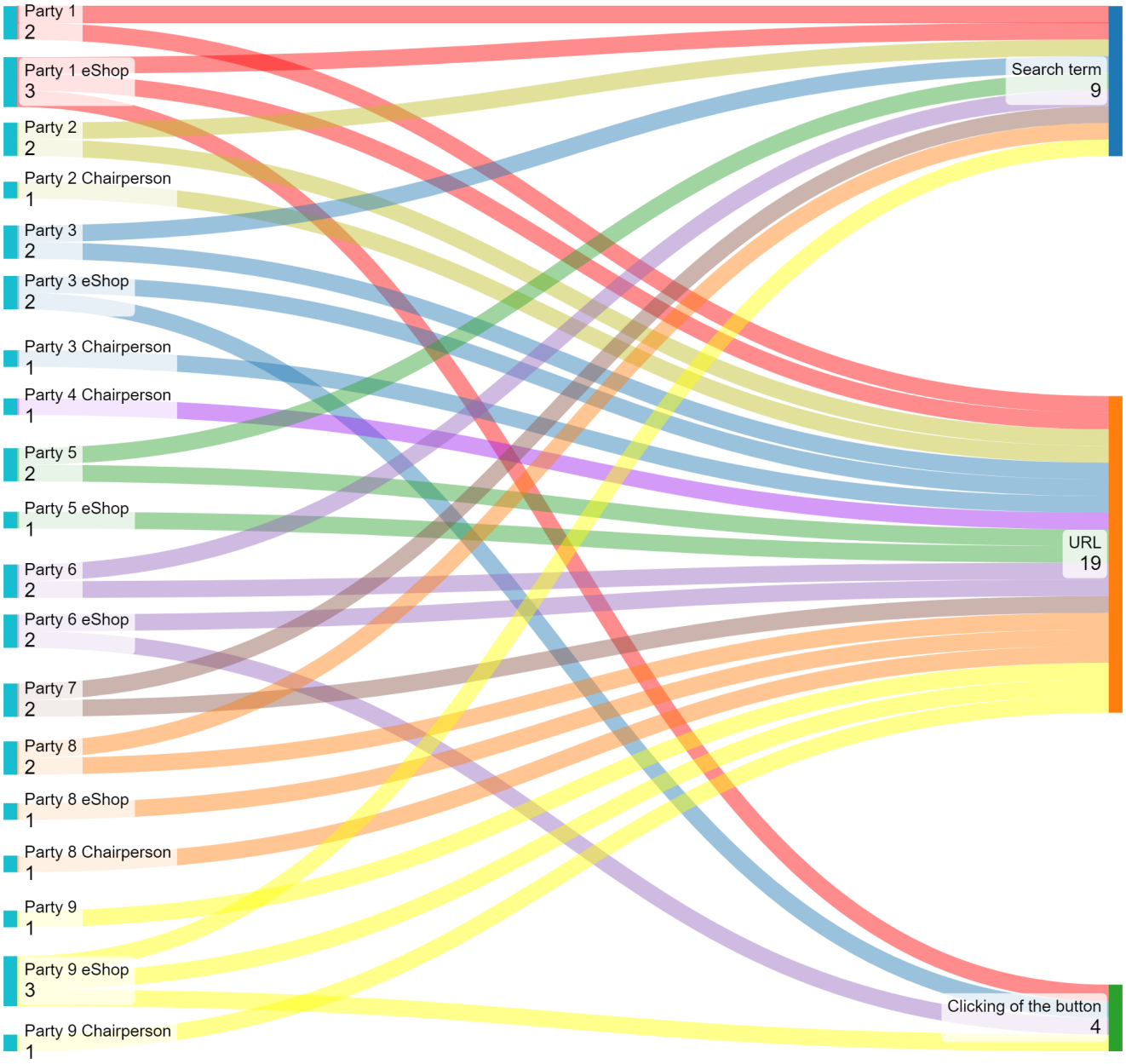

Figure 2: Leaks of specific data items per party. Every data item leakage increments the number of leaked items in a site and the sum of every leaked item. A connection to a specific third-party service is counted only once even if several data items are leaked to it by a website.

kind of phenomena in the first place, not advance it. Their websites should be held to a higher standard of privacy than any normal organization, association or private company.

It is not surprising that in this research the majority of data leaks were caused by Google Analytics, or that Meta Pixel followed closely behind it. These two actors, and especially Google Analytics, have been proven time and again to be the main culprits for the personal data leaks [21]. They are also the most widely used analytics tools globally, which is a position that further feeds their usage regardless of the fact that they are not exactly optimal regarding the website user privacy. While it is not possible to know whether the collected sensitive personal data is being stored and used, the fact that is sent to these large analytics companies is by itself alarming.

Our investigation to the dark patterns showed that the use of these kinds of design choices is, unfortunately, rife on the political party websites just as much as everywhere else on the internet. One notable pattern emerged, though, and it was the complete lack of cookie consent banners which was exhibited in 38.5% of the studied websites. Since obtaining valid consent is mandated by the GDPR for all websites that use any kinds of cookies, the lack of cookie consent banners in such a high proportion is truly astounding. Especially for parties with ample legal resources, claiming ignorance of the GDPR or lacking advisors to point out such failings is unthinkable. One possible explanation for the lack of cookie consent banners might be that many of these websites have been in existence far longer than the GDPR has, and perhaps this situation is purely an unfortunate oversight on the part of maintainers of the websites.

From the perspective of avoiding these kinds of leakages in future, we would advice the developers building and maintaining these websites to follow certain development practices. Firstly, all network traffic should be analyzed in the way that we have done in this study. It requires neither special expertise nor great investment of time, making arguments against doing so moot. Analytical tools that are found to leak data to third parties should be removed. And if the use of website analytics is deemed absolutely necessary, solutions that can be deployed locally, so that there is no risk of this kind of leakages happening in the first place, should be favored.

6 CONCLUSIONS

In this study, we have surveyed the websites of major political parties of Finland, and found that all of the parties leak personal data to third parties through at least one of their affiliated websites. Considering the nature of these websites, this data may often reveal the user's political opinion combined with their identity. Most often the data is leaked to Google and Meta, although smaller actors in the field of data analytics are also present. Data leaks and breaches of user privacy on politically motivated websites raise several concerns and casts the political parties of Finland in an unbecoming light.

ACKNOWLEDGMENTS

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

REFERENCES

[1] Vibhor Agarwal, Yash Vekaria, Pushkal Agarwal, Sangeeta Mahapatra, Shounak Set, Sakthi Balan Muthiah, Nishanth Sastry, and Nicolas Kourtellis. 2021. Under the Spotlight: Web Tracking in Indian Partisan News Websites. In *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 15. 26–37.

[2] Colin Bennett. 2013. The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies. *Elections and Voter Surveillance in Western Democracies (June 15, 2013)* (2013).

[3] Colin J. Bennett. 2016. Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America? *International Data Privacy Law* 6, 4 (12 2016), 261–275. https://doi.org/10.1093/idpl/ipw021 arXiv:https://academic.oup.com/idpl/article-pdf/6/4/261/9598014/ipw021.pdf

[4] Benjamin Maximilian Berens, Mark Bohlender, Heike Dietmann, Chiara Krisam, Oksana Kulyk, and Melanie Volkamer. 2024. Cookie disclaimers: Dark patterns and lack of transparency. *Computers & Security* 136 (2024), 103507.

[5] Benjamin Maximilian Berens, Heike Dietmann, Chiara Krisam, Oksana Kulyk, and Melanie Volkamer. 2022. Cookie Disclaimers: Impact of Design and Users' Attitude. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*. 1–20.

[6] Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig, and Gabriele Lenzini. 2021. " I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!"-Dark Patterns from the End-User Perspective. In *Designing Interactive Systems Conference 2021*. 763–776.

[7] Ida Borberg, Rene Hougaard, Willard Rafnsson, and Oksana Kulyk. 2022. So I Sold My Soul": Effects of Dark Patterns in Cookie Notices on End-User Behavior and Perceptions. In *Workshop on Usable Security and Privacy (USEC)*, Vol. 3.

[8] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the dark side: privacy dark strategies and privacy dark patterns. *Proc. Priv. Enhancing Technol.* 2016, 4 (2016), 237–254.

[9] Corina Cara et al. 2019. Dark patterns in the media: A systematic review. *Network Intelligence Studies* 7, 14 (2019), 105–113.

[10] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3174108

[11] Philip N Howard and Daniel Kreiss. 2009. Political parties & voter privacy: Australia, Canada, the United Kingdom, and United States in comparative perspective. *Howard, Philip N., and Daniel Kreiss* (2009).

[12] Emre Kocyigit, Arianna Rossi, and Gabriele Lenzini. 2022. Towards Assessing Features of Dark Patterns in Cookie Consent Processes. In *IFIP International Summer School on Privacy and Identity Management*. Springer, 165–183.

[13] Chiara Krisam, Heike Dietmann, Melanie Volkamer, and Oksana Kulyk. 2021. Dark Patterns in the Wild: Review of Cookie Disclaimer Designs on Top 500 German Websites. In *Proceedings of the 2021 European Symposium on Usable Security* (Karlsruhe, Germany) *(EuroUSEC '21)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3481357.3481516

[14] Aditi M. Bhoot, Mayuri A. Shinde, and Wricha P. Mishra. 2020. Towards the identification of dark patterns: An analysis based on end-user reactions. In *Proceedings of the 11th Indian Conference on Human-Computer Interaction*. 24–33.

[15] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 81 (nov 2019), 32 pages. https://doi.org/10.1145/3359183

[16] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 360, 18 pages. https://doi.org/10.1145/3411764.3445610

[17] Arvind Narayanan, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. 2020. Dark Patterns: Past, Present, and Future: The Evolution of Tricky User Interfaces. *Queue* 18, 2 (may 2020), 67–92. https://doi.org/10.1145/3400899.3400901

[18] Sebastian Stier Nora Kirkizh, Roberto Ulloa and Jürgen Pfeffer. 2024. Predicting political attitudes from web tracking data: a machine learning approach. *Journal of Information Technology & Politics* 0, 0 (2024), 1–14. https://doi.org/10.1080/19331681.2024.2316679 arXiv:https://doi.org/10.1080/19331681.2024.2316679

[19] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376321

[20] Timothy Richards and A. Ant Ozok. 2018. Trust Building Privacy Preferences for Young Adults Visiting Political Campaign Websites. In *Advances in Communication of Design*, Amic G. Ho (Ed.). Springer International Publishing, Cham, 52–63.

[21] Nayanamana Samarasinghe, Aashish Adhikari, Mohammad Mannan, and Amr Youssef. 2022. Et tu, Brute? Privacy Analysis of Government Websites and Mobile Apps. In *Proceedings of the ACM Web Conference 2022* (, Virtual Event, Lyon, France,) *(WWW '22)*. Association for Computing Machinery, New York, NY, USA, 564–575. https://doi.org/10.1145/3485447.3512223

[22] Esko Vuorinen, Panu Puhtila, Sampsa Rauti, and Ville Leppänen. 2023. From Whistle to Echo: Data Leaks in Web-Based Whistleblowing Channels. In *Nordic Conference on Secure IT Systems*. Springer, 37–53.

[23] Ari Ezra Waldman. 2020. Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology* 31 (2020), 105–109. https://doi.org/10.1016/j.copsyc.2019.08.025 Privacy and Disclosure, Online and in Social Interactions.