Leaky Democracy: Third Parties in Voting Advice Applications

Timi Heino[1], Sampsa Rauti[1], Samuli Laato[1], Robin Carlsson[1], and Ville Leppänen[1]

University of Turku, 20014 Turku, Finland
tdhein,sjprau,sadala,crcarl,ville.leppanen@utu.fi

Abstract. An important part of democracy is the premise of ballot secrecy, where each individual can vote privately without interference, and without anyone getting to say what they vote for. Legislation such as GDPR also indicates that a person's political opinion is sensitive personal data. Yet, in the modern technological era, there are countless ways through which people's political views can be probed, stored and in the worst cases, manipulated. One avenue through which this can happen are voting advice applications, online tools designed for helping people in selecting optimal candidates during elections. In this work, we performed a network traffic analysis of Finnish voting advice applications during the parliamentary election of Spring 2023, to see whether any sensitive information regarding, for example, the persons' political opinions, is leaked to third parties through the available voting advice applications. The results revealed that in 7 out of 11 analyzed applications, this was the case. Our work offers empirical evidence showing that while there may still be secrecy in the voting booth, the steps leading to the booth are paved with data leaks. We conclude the study by discussing the assurance of democratic processes and systems in our modern socio-digital society.

Keywords: Voting advice applications · third-party services · online privacy

1 Introduction

Today, the internet is an important tool in politics, having transformed the way people obtain information and participate in politics. It has changed the way political campaigns are run, and transformed how people interact with candidates and parties. Arguably, voters now have access to more information about candidates and their history, and have the ability to make more informed decisions before voting. Furthermore, there are websites and applications designed to aid participants in making informed decisions. Voting advice applications and political party websites are prime examples of this digital transformation [10, 16].

Voting advice applications are digital tools that help voters make informed decisions during an election. These applications are prominently online, and

became available in Europe in the early 2000s to promote awareness among citizens during electoral campaigns [17]. They typically first create a set of questions (concerning various contemporary political issues) and ask political candidates to respond to these questions. They then provide users with the same questions, and based on the user's answers, the application then creates a list of political parties or candidates compatible with the user's views. Other supporting information, e.g., regarding the positions and policies advocated by those parties or candidates, can also be displayed. The main disclosed goal of these applications is to make the process of choosing a candidate accessible and transparent by providing voters with comprehensible information [1]. They can also help voters overcome cognitive biases or misinformation that may affect their decisions. Ideally, voting advice applications can offer the user an objective and data-driven analysis of political positions, and encourage them to make more thoughtful decisions [2].

In Finland, for example, the use of voting advice applications has surged in recent years. Statistics Finland reported in 2019 that nearly half (49%) of eligible voters in the country used one or several voting advice applications during the election season [26]. According to this report, voting advice applications have now become one of the primary means of gaining knowledge about candidates. The situation seems to be similar in many technologically developed countries across Europe. For example, in the Netherlands, a single voting advice application named "Stemwijzer" was used 4 million times during elections, which corresponds to more than 50% of Dutch voters [22].

As the use of voting advice applications has gained popularity, modern websites have also grown increasingly complex and regularly make use of various third-party services such as pre-made plugins for improved functionality and web analytics [31, 23, 30]. Understanding user behavior through analytics and employing ready-made third-party components gives many benefits to website maintainers, but it also raises serious concerns when it comes to confidentiality and privacy. If developers are not careful, website users' sensitive personal data can be sent to these third-parties. This has repeatedly shown to be the case even in many essential web services and public sector websites [12, 28].

Majority of the studies on voting advice applications seem to focus on impact, models and algorithms of these applications [1, 8, 25, 21, 29]. These are important issues, but at the same time, online privacy concerns are currently largely omitted in this field of research. Kaskina et al. [15] presented a study introducing a privacy framework for protecting their political profile and affiliations from other users of voting advice applications in a setting where a voting advice application is seen as a social platform enabling interaction and political discussion with other users. However, the authors do not discuss means for avoiding leaks to third parties such as analytics services.

To the best of our knowledge, the current paper is the first study to specifically address the privacy of voting advice applications from the software engineering point of view. Therefore, this study fills the gap in the research on voting advice application privacy and, in particular, privacy issues caused by

third-party analytics. By performing a network traffic analysis on 11 Finnish voting advice applications, we show that these applications leak sensitive data on users' political opinions to third parties such as Google and Meta, which is a great concern from both technological and political perspectives.

The remainder of this paper is organized as follows. Section 2 provides more background on privacy of political opinions. Section 3 describes the selection of the studied voting advice applications, and the network traffic analysis we performed. Section 4 presents the results, describing the data leaks found in the applications. Section 5 discusses the implications of our findings both from political and technical perspectives. Finally, Section 6 concludes the paper.

2 Privacy of political opinions

The practice of secret ballots was first used in the Roman assemblies in the second century in order to diminish the power of the upper classes over the eligible voters, thus allowing citizens greater freedom of choice [11]. As Cicero stated, "everyone knows that laws which provide a secret ballot have deprived the aristocracy of all its influence." [19, p. 268] The similar reasoning was used in the United States by the advocates of secret ballots. Implementing secret ballots was seen as a solution to combat the problem of coercion and bribery [14]. It promotes a fair and unbiased electoral process and allows voters to cast their votes without fear of retaliation [20]. Today, confidentiality of ballots is seen as a fundamental characteristic of legitimate elections, and Article 25 of the United Nations' Civil and Political Covenant acknowledges the significance of the secret ballot as a prominent element of a just and fair electoral system.

While ballot secrecy might be the culmination point when it comes to privacy of political opinion, privacy is also important before the actual voting to ensure freedom from coercion and adverse influencing. This is also true when it comes to voting advice applications. The same sentiment is also reflected in the General Data Protection Regulation (GDPR): data on political opinions is considered sensitive personal data (special category data) [6]. When the data on political opinions is shared with third parties, the user should grant explicit consent for this or there has to be a lawful basis for sharing. Additionally, the user should be adequately informed of the purpose of the data processing and the categories of personal data being processed. The user should also learn the identity of the third parties receiving the data.

One prominent example of the dangers data leaks pose to democracy is the Cambridge Analytica scandal. In 2018, it was revealed that Facebook had handed over identifiable personal data of more than 87 million users to a British political consulting firm, Cambridge Analytica [13]. Voter profiles were built using the data and targeted advertisements were placed on Facebook and other online platforms in order to sway voters' opinions [3]. This caused a public outcry over the misuse of personal data and increased concerns about online data leaks and the impact targeted political advertisements can have on democratic elections.

3 Method

We studied 11 popular Finnish voting advice applications. While there appears to be no accurate statistics of popularity of voting advice applications, we aimed to choose applications provided by the largest media outlets in Finland, as well as applications having a high ranking in Google results. The media outlets or organizations offering the selected applications are anonymously described in Table 1. The goal was not to cover all Finnish voting advice applications, but rather to choose some popular ones to demonstrate that third-party services pose a serious threat to privacy of political opinion when using the applications.

Table 1. The applications and descriptions of media outlets and organizations providing these services

Application	Provider description
VAA 1	An online job search platform
VAA 2	A Finnish daily newspaper
VAA 3	A daily tabloid newspaper
VAA 4	A regional newspaper
VAA 5	A daily tabloid newspaper
VAA 6	A regional newspaper
VAA 7	A regional newspaper
VAA 8	A commercial television channel
VAA 9	A regional newspaper
VAA 10	The national public broadcasting company of Finland
VAA 11	Finnish National Youth Council

Our experiment involved testing the voting advice applications by first choosing an electoral district (Varsinais-Suomi was chosen) or municipality (Turku), completing the questionnaire and opening the page of the top candidate recommended by the application. All cookies were accepted upon accessing the studied websites. We recorded the network traffic with Google Chrome's Developer Tools. Caching was turned off and the traffic was filtered so that only the requests going to third parties were analyzed. The recorded traffic was stored as a log file for further analysis. We then analyzed the payloads of all third-party web requests. Any data that could be interpreted as a political opinion (in the case of voting advice applications, this usually means either the information about top candidates or answers to political questions) and was sent to third parties was extracted from the log file.

We also analyzed the privacy policies of the websites on which the selected voting advice applications were found – or, in case a studied application had its own privacy policy, we studied this document. The privacy policies were searched for mentions of sharing data on political opinion to third parties. We also investigated whether the documents named the third parties that – according to

our previous network traffic analysis – received sensitive personal data from the website.

4 Results

Figure 1 shows an alluvial diagram of the data flows from voting advice applications to third parties. The diagram only shows the data flows where data on the user's political opinion was leaked. We can see that most of the studied applications, 7 in total, leaked this data. In all 7 cases, this happened by leaking the information on the candidate pages the user visited after getting the results on top candidates. When the user visits the pages of the top candidates, the third parties receive the page URL. The URL often contains the candidate's name directly, but even if it does not, the information about the candidate can be considered to be leaked because the third party can simply visit the candidate page to further analyze it. This kind of analysis can easily be automatized with the help of AI.

When looking at the applications, we can see that Voting advice application 1, provided a Finnish online job search platform, leaks the information about top candidates to 7 different third parties, which is nearly half of all unique third parties found in the current study! Voting advice application 7 provided by a Finnish media company does not do much better: top candidates viewed by the user are leaked to 6 third parties. Voting advice applications 2, 3, and 4 all leak the viewed candidates to 3 third parties. These media outlets are all owned by the same Finnish media company, which explains why they have the same third parties in their applications. Voting advice applications 5 and 6 leak top candidates to 2 third-parties. Finally, there were four voting advice applications (applications 8, 9, 10 and 11) where no leaks of political opinions were detected.

Figure 1 also shows the third parties involved. The fact that Google, with its various tools and services, is the most frequently found third party is hardly surprising – 5 voting advice applications leak political opinions to Google. Meta, UserReport (a tool for gathering user feedback) and Giosg (a live chat tool) are present in 3 applications. Chartbeat, a content intelligence platform providing data and analytics for publishers, has 2 instances. Finally, there are miscellaneous third parties that are only found once in the analyzed applications. Many of these services, such as Adform, AppNexus, Rubicon Project, Smart Adserver and OneTag Advertising System, are related to online advertising. There are also several well-known social media platforms like LinkedIn, Snapchat, TikTok and Twitter, as well as New Relic, which provides performance monitoring and optimization tools. While all of these third parties may not actively and knowingly collect sensitive user data such as political opinions, it is clear that this information should not end up on their servers to begin with.

It is worth noting that the data sent to third parties, along with political opinions of users, contains technical details like IP addresses, and device and user specific identifiers. There are also many other technical pieces of information such as the screen size, operating system and browser along with their versions,

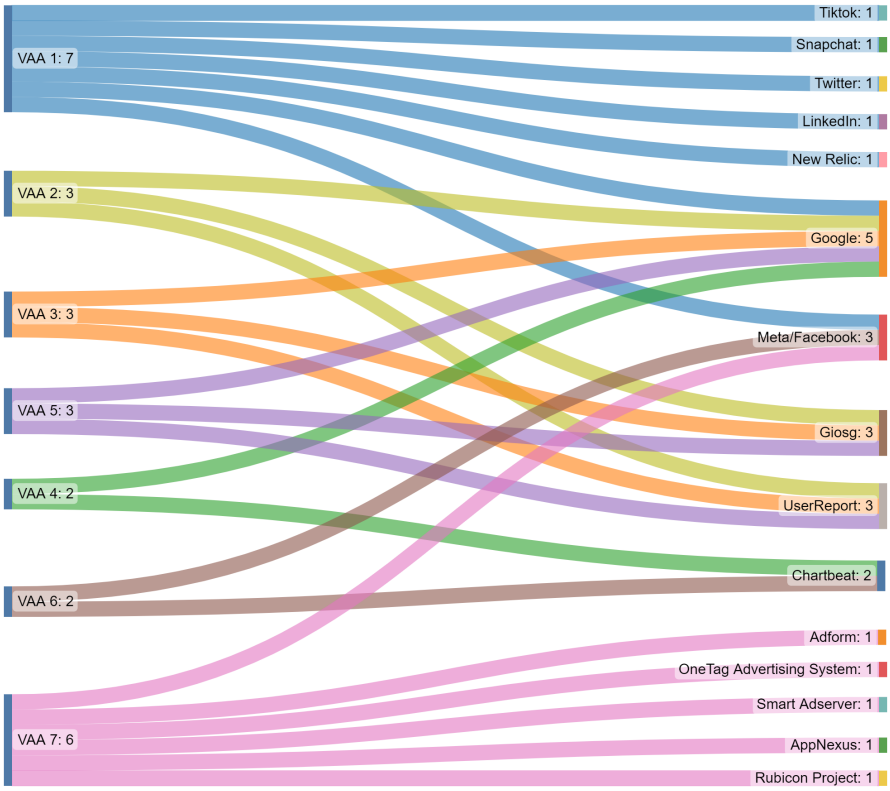

Fig. 1. An alluvial diagram showing the flows of sensitive political data from voting advice applications to third parties.

and so forth. It is safe to assume large analytics service providers usually know who the user is, and consequently, whom the sensitive political data belongs to.

When it comes to privacy policies of the analyzed applications, none of the 7 applications leaking political opinions mentioned this in their privacy policies. While the used third-party services were mentioned in privacy policies, the user does not get a clear understanding what kind of data is sent to third parties. Therefore, it can be argued that the user does not get appropriately informed in these cases. Also, only providers of Voting advice applications 2, 3, and 4 specifically addressed the voting advice application in their privacy policies. Other privacy policy documents were more general and did not separately address the application.

5 Discussion

We have seen that the majority of the studied voting advice applications leak the candidates viewed by the user to third parties. When political opinions of users leak to third parties without clear consent, this can have adverse effects on democracy. Privacy of political opinions, usually deemed a fundamental principle in democratic elections, is jeopardized. If voters have reason to believe that their political opinions are no longer private, they can be afraid of expressing their actual beliefs and opinions. Jeremy Bentham, a philosopher and founder of modern utilitarianism, argued that disclosing an individual's vote can undermine the accuracy of their expression of political will [27]. Therefore, privacy leaks can result in a distortion of the election outcome.

The GDPR is somewhat vague about the meaning of the term "political opinion". It can be interpreted to mean a political ideology (e.g. liberal, conservative), more specific political party affiliation, or stances on various policies (economical, environmental etc.) [4]. Although the definition is not completely clear, the voting advice applications can leak political information in all of the above categories. If a third party gets a couple of the top candidates returned to the user by the application, political ideology and party affiliation can be deduced. Moreover, even some opinions on policies may be approximately determined by looking at the answers by the user's top candidates. In the light of the previously discussed Cambridge Analytica scandal and continuously increasing political microtargeting where malleable voters are targeted with highly personalized messages [5], the privacy of these applications should be a high priority. If political opinions leak to third parties, public opinion can be manipulated by large companies, foreign powers, political actors, or different interest groups. Consequently, elections may no longer be "fair and free" in the sense that Robert Dahl, one of the most influential political theorists of the 20th century, considered to be characteristic of democracy [7, p. 233].

From a software engineering point of view, a significant factor contributing to the privacy problem is the fact that many media outlets do not seem to treat their voting advice applications any different from their main website, which means the special nature of personal data concerning political opinions is not given

necessery attention. The websites of media outlets often make use of different software platforms which in turn may contain third-party web analytics or at least make enabling them effortless by offering plugins for this purpose. Analytics are then also enabled for voting advice applications without fully appreciating the privacy consequences.

While letting personal data on political opinions leak to third parties is likely to be completely unintentional, the implications can be very serious, as demonstrated by the previously mentioned Cambridge Analytica case. Therefore, website developers and data protection officers should always be aware of what kind of data flows from their websites to third parties. This is not a difficult task – at least the most critical functionalities on a website could be inspected with an experimental setup similar to the one employed in the current study. Such analysis should be an essential part of any web development project dealing with sensitive personal data. It is also important to carefully justify the use of each analytics service, and when analytics are deemed necessary, developers should look into alternatives that store data locally (e.g. by using an open source solution such as Matomo [9]). This way, the data remains under the control of the organization or media outlet, and will not be surrendered to a third party.

By looking at our findings, it is also apparent that the media outlets and other providers of voting advice applications have failed to create clear and transparent privacy policy documents. Sadly, this is a common problem in today's web services [18]. The privacy policy documents we studied did not, for the most part, provide appropriate information about data processing activities. On large websites, addressing services such as voting advice applications separately in a privacy policy – or creating own privacy policy documents for these services – would be very important. Transparently addressing third parties in the privacy policy would no doubt also make the maintainers of a voting advice application think twice whether it is wise to use third-party analytics services at all. Moreover, using standardized templates when writing privacy policies could make them easier to create and understand [24].

6 Conclusions

We have presented an overview of data leaks in Finnish voting advice applications. Although our dataset does not cover all Finnish voting advice applications, the finding that 7 out of 11 studied applications leak sensitive political data is alarming. In future, voting advice applications in other countries should also be exposed to the same kind of network traffic analysis. Data leaks to third parties could also be further analyzed by testing voting advice applications with different consent choices.

Hopefully, our results serve as a reminder to software developers and data protection officers responsible for web services that handle sensitive data. Service operators have to understand their accountability for keeping the users' personal data safe and clearly informing users of what personal data is processed and what third parties are involved. In web applications processing sensitive political data,

it is difficult to find valid justifications for the use of external web analytics services. Users should be able to trust that their political opinions stay safe when looking for information about candidates and parties.

Acknowledgements

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

References

1. Alvarez, R.M., Levin, I., Trechsel, A.H., Vassil, K.: Voting advice applications: How useful and for whom? Journal of Information Technology & Politics **11**(1), 82–101 (2014)
2. Andreadis, I.: Voting advice applications: a successful nexus between informatics and political science. In: Proceedings of the 6th Balkan Conference in Informatics. pp. 251–258 (2013)
3. Bakir, V.: Psychological operations in digital political campaigns: Assessing cambridge analytica's psychographic profiling and targeting. Frontiers in Communication **5**, 67 (2020)
4. Bennett, C.: The Politics and the Privacy of Politics: Parties, Elections and Voter Surveillance in Western Democracies. First Monday (8) (2013)
5. Blasi Casagran, C., Vermeulen, M.: Reflections on the murky legal practices of political micro-targeting from a gdpr perspective. International Data Privacy Law **11**(4), 348–359 (2021)
6. Cabañas, J.G., Cuevas, Á., Cuevas, R.: Unveiling and quantifying facebook exploitation of sensitive personal data for advertising purposes. In: 27th {USENIX} Security Symposium ({USENIX} Security 18). pp. 479–495 (2018)
7. Dahl, R.A.: Democracy and its Critics. Yale university press (2008)
8. Fivaz, J., Nadig, G.: Impact of voting advice applications (VAAs) on voter turnout and their potential use for civic education. Policy & Internet **2**(4), 167–200 (2010)
9. Gamalielsson, J., Lundell, B., Butler, S., Brax, C., Persson, T., Mattsson, A., Gustavsson, T., Feist, J., Lönroth, E.: Towards open government through open source software for web analytics: The case of matomo. JeDEM-eJournal of eDemocracy and Open Government **13**(2), 133–153 (2021)
10. Garzia, D., Marschall, S.: Voting advice applications. Oxford University Press (2019)
11. Gerber, A.S., Huber, G.A., Doherty, D., Dowling, C.M.: Is there a secret ballot? Ballot secrecy perceptions and their implications for voting behaviour. British Journal of Political Science **43**(1), 77–102 (2013)
12. Heino, T., Carlsson, R., Rauti, S., Leppänen, V.: Assessing discrepancies between network traffic and privacy policies of public sector web services. In: Proceedings of the 17th International Conference on Availability, Reliability and Security. pp. 1–6 (2022)
13. Isaak, J., Hanna, M.J.: User data privacy: Facebook, cambridge analytica, and privacy protection. Computer **51**(8), 56–59 (2018)
14. Kam, C.: The secret ballot and the market for votes at 19th-century British elections. Comparative Political Studies **50**(5), 594–635 (2017)

15. Kaskina, A., Meier, A.: Integrating privacy and trust in voting advice applications. In: 2016 Third International Conference on eDemocracy & eGovernment (ICEDEG). pp. 20–25. IEEE (2016)
16. Kruikemeier, S., Aparaschivei, A.P., Boomgaarden, H.G., Van Noort, G., Vliegenthart, R.: Party and candidate websites: A comparative explanatory analysis. Mass Communication and Society **18**(6), 821–850 (2015)
17. Mahéo, V.A.: Information campaigns and (under) privileged citizens: An experiment on the differential effects of a voting advice application. Political Communication **34**(4), 511–529 (2017)
18. Mulder, T.: Health apps, their privacy policies and the gdpr. European Journal of Law and Technology (2019)
19. Nicolet, C.: The World of the Citizen in Republican Rome (1988)
20. Orr, S., Johnson, J., Mitchell, J.: Secret Ballots and the Promotion of Democratic Ideals: Strategic Structure and Normative Justification. Political Studies Association (2018)
21. Otjes, S., Louwerse, T.: Spatial models in voting advice applications. Electoral Studies **36**, 263–271 (2014)
22. Pajala, T., Korhonen, P., Malo, P., Sinha, A., Wallenius, J., Dehnokhalaji, A.: Accounting for political opinions, power, and influence: a voting advice application. European Journal of Operational Research **266**(2), 702–715 (2018)
23. Quintel, D., Wilson, R.: Analytics and privacy. Information Technology and Libraries **39**(3) (2020)
24. Rowan, M., Dehlinger, J.: A privacy policy comparison of health and fitness related mobile applications. Procedia Computer Science **37**, 348–355 (2014)
25. Schultze, M.: Effects of voting advice applications (VAAs) on political knowledge about party positions. Policy & Internet **6**(1), 46–68 (2014)
26. Statistics Finland: Puolet äänioikeutetuista käytti vaalikonetta ennen eduskuntavaaleja. https://www.stat.fi/til/sutivi/2019/sutivi_2019_2019-11-07_kat_002_fi.html (2019)
27. Theuns, T.: Jeremy Bentham, John Stuart Mill and the secret ballot: Insights from nineteenth century democratic theory. Australian Journal of Politics & History **63**(4), 493–507 (2017)
28. Thompson, N., Ravindran, R., Nicosia, S.: Government data does not mean data governance: Lessons learned from a public sector application audit. Government information quarterly **32**(3), 316–322 (2015)
29. Wagner, M., Ruusuvirta, O.: Faulty recommendations? Party positions in online voting advice applications. Party Positions in Online Voting Advice Applications (2009)
30. Wambach, T., Bräunlich, K.: The Evolution of Third-Party Web Tracking. In: Camp, O., Furnell, S., Mori, P. (eds.) Information Systems Security and Privacy. pp. 130–147. Springer International Publishing (2017)
31. Zheutlin, A.R., Niforatos, J.D., Sussman, J.B.: Data-tracking on government, nonprofit, and commercial health-related websites. Journal of general internal medicine pp. 1–3 (2021)