ORG OPEN RIGHTS GROUP

MORAL HAZARD
VOTER DATA PRIVACY AND POLITICS IN ELECTION CANVASSING APPS

January 2025

ABOUT ORG

Open Rights Group (ORG) is a UK based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. We are a grassroots organisation with supporters and local groups across the UK.

Our work on data protection and privacy includes challenging the immigration exemption to UK data protection law, defending the General Data Protection Regulation (GDPR) from attempts to water down its provisions, and challenging uncontrolled and unlawful data sharing by online advertisers.

openrightsgroup.org

Report by: **Jacob Ohrvik-Stott**

Data Protection Consultant: **Jim Killock**

Technical Researcher: **Paul May**

EXECUTIVE SUMMARY

In this report we analyse the technical architecture, and associated privacy policies, of the canvassing apps used by the Liberal Democrat, Conservative, and Labour parties during the 2024 general election. The legal and ethical use of such canvassing data is critical for protecting the integrity of elections, and by extension democracy.

The UK's political parties are seemingly caught in a data arms race, where the stakes and pace of electoral politics may be driving them to cut governance corners. A lack of transparency around how people's sensitive data is used poses the risk of creating a chilling effect on voters. Private companies may claim grounds on which they can monetise voter data which is willingly handed over by canvassers of UK political parties, in return for perceived competitive advantage.

Our analysis of apps shows that concerns around privacy and security are already very significant. Our Static Application Security Testing analysis of the Liberal Democrat's *MiniVan* App found that it was deployed with infrastructure with a history of security vulnerabilities. An analysis of Labour's web-based *Reach*, *Doorstep* and *Contact Creator* apps found these apps were integrated with infrastructure owned by Experian. The Conservatives' *Share2Win* app also presented security vulnerabilities and access to data that would raise privacy concerns, such as location tracking. All parties – including the Conservatives through their *Share2Win* and *VoteSource* App – appear to be reliant on international commercial entities to run their digital campaigning infrastructure.

Open Rights Group's 2020 *Who Do They Think We Are?* research found the UK's major political parties engaged in extensive problematic profiling of the electorate, enabled by questionable relationships with major data brokers such as Experian. Similar themes echo throughout this report, where our analysis raises questions around how secure these apps are, and if the public's data is being unlawfully shared with commercial organisations.

Power asymmetries between parties and providers potentially make it harder for parties to assert control over how apps are designed. Limited resources and curtailed delivery schedules also increase privacy and security risks, by paying less regard than necessary to data protection law.

This report comes at a point where the current Data (Use and Access) Bill has removed proposals to extend the use of data for political campaigning purposes which were contained in the previous changes proposed by the Conservative administration. This is very welcome, but is undermined by the ease with which a future secretary of state could reintroduce wide use of data through Statutory Instrument, known as "Henry VIII powers".

The ability of a secretary of state to change the rules around electoral data creates the possibility that new uses of data could be legitimised shortly before an election, changing the electoral game with short timescales to adapt technologies to take advantage: both a moral hazard for any future government, and a security and privacy nightmare.

To address this uncertainty around problematic canvassing app data sharing, and build much-needed trust in electoral processes, we recommend:

1. **Political parties must urgently publish in the full list of organisations they share canvassing data with.** Our research suggests some parties only refer to generic organisation types (e.g. "commercial partners"), whilst others do not appear to have listed the organisations our technical analysis suggests are involved in supporting canvassing apps.

2. **Political parties should collectively agree to publish financial details of agreements with commercial providers to provide canvassing infrastructure.** This would help to highlight any deals where data assets implicitly form part of the value of a commercial agreement (for example where data brokers provide free access to infrastructure in exchange for data access).

3. **Political parties should proactively publicly publish canvassing data protection policies to maintain trust** – for example publishing DPIAs for canvassing apps, specific data sharing agreements with third parties, and privacy consent forms provided to voters. Our research team could find no public evidence of such materials, beyond general privacy policies and some partial information within app user manuals.

4. **The ICO and Electoral Commission develop new "anticipatory" regulatory assurance programmes that ensure political campaigning is lawful before and during elections** – not retrospectively after they have concluded and damage is already done. This could include the ICO delivering a regulatory sandbox scheme or committing to proactive assurance audits for all major political parties' canvassing apps.

5. **The current Labour government should introduce new measures to strengthen governance of political canvassing and opinion data under the DUA Bill and election reform agenda**. This will deliver on their commitment in the King's Speech to "strengthen the integrity of elections". Reforms should include mandatory public publication of political opinion data sharing agreements, and outlawing the use of canvassing data for commercial benefit.

6. **The ICO investigates if and how data has been shared between Labour and Experian throughout the 2024 election period**. This is critical given the various potential data protection compliance issues and risks raised by our investigation, and the history of regulatory activity focused on Experian and political campaigning.

7. **The ICO should provide explicit guidance that sharing of election canvassing data with third parties constitutes "large-scale" processing of special category data** – meaning it is high risk processing under the UK GDPR, and heightened safeguards and DPIAs are required. This should remain the case even where data is pseudonymised.

8. **The government's proposed Integrity and Ethics Commission should investigate the relationships between data brokers and elected officials** as a priority – recognising that transfer of data to third parties is essentially transfer of money given the significant value of these datasets, and should therefore be held to the same public standards and levels of scrutiny as financial interests.

1 INTRODUCTION

Since our inception, Open Rights Group (ORG) has defended the UK's democratic system, working to ensure elections are fair and open and political parties act legally and ethically. In 2020, our *Who do they think we are?* report lifted the lid on how political parties trade and grade the personal data of our citizens to serve their own interests. We showed how all political parties attempted to profile both personal information and highly protected 'special category data' such as religious and political opinion data, and ethnicity. They exploited legal grey areas in UK data protection law, undermining the integrity of elections in the process.

This report builds on this work, taking a closer look at how the personal data within political parties' canvassing apps is governed and shared. Our findings pose urgent questions about potential problematic data misuse, and unethical relationships between the organisations involved. The themes discussed in the third section of this report are all-too-familiar, echoing previous ORG complaints that called political parties' involvement with Experian into question.[1] That these questions remain open points to a need for regulators to do more to foster transparency and trust. If data is being used lawfully they should confirm this by proactively investigating or compelling parties to publish more public information on canvassing app governance. If data is being misused, they should take strong action to uphold public trust in political parties.

In particular, the Information Commissioner's Office (ICO) should make sure that its guidance on the use of personal data in political campaigning[2] is being followed. This guidance places the onus on political parties to conduct "rigorous checks" on third parties providing marketing data services, to ensure they comply with all aspects of data protection law. This includes confirming individuals' have been told exactly how their data could be used and provided informed consent, and ensuring that any third parties accessing this data have been explicitly identified (in the words of the ICO *"it is not sufficient [to refer to data sharing recipients] in a general sense, eg 'selected third parties', 'trusted partners'"*). But the recent reprimand issued by the ICO to the Labour Party[3] suggests political parties are still struggling with the basics of data protection compliance: the party's "privacy inbox" had not been monitored for three years, and over three quarters of individuals' Subject Access Requests had not received a response within the maximum compulsory time limit of three months.

---

1 Leaks to Sky News in 2019 revealed that the Conservative Party categorises people using Experian's VoteSource database, which used over 850 million records to classify people into 66 personas based on various factors such as crime data, GCSE results, and gas and electricity consumption. The same leak revealed that the Labour party used Experian's Mosaic database and Experian Origin tool, that allowed them to target voters based on ethnicity with classifications such as "Black African," "Celtic," and "Jewish/Armenian."
The Open Rights Group registered a complaint about these activities: https://www.openrightsgroup.org/app/uploads/2021/01/Rice-Crowe-Killock-Haydock-v-Labour-Conservatives-Lib-Dems-ICO-Complaint-11-December-2020-core-arguments.pdf ;
https://news.sky.com/story/data-protection-experts-want-watchdog-to-investigate-conservative-and-labour-parties-11845278

2 Source: https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1/

3 Source: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/08/action-taken-against-labour-party-for-failing-to-respond-to-requests-for-personal-information-on-time/

This report also speaks to bigger-picture tensions in the relationships between regulators, political parties, government, and NGOs. The pace at which elections are conducted seemingly results in a data arms race between parties, where inadequate governance is an acceptable price to pay for keeping up with political rivals' campaigning capabilities. This competitive pressure also creates potential incentives to generate party funds through suspect data practices. In April 2024 it was reported that the Conservative party considered allowing commercial organisations access to its membership database for geo-targeted advertising in exchange for a portion of the revenue – although a party spokesman said the idea "did not progress beyond the pitch stage".[4]

Upholding data governance standards is made more challenging by the difficulties regulators face when making demands of a government that can legislate to change data protection laws. This can be seen in the current moment, where the Digital Information and Smart Data (DSID) Bill reforms are likely to generally promote increased data portability and public-private data sharing. For Open Rights Group and organisations like ourselves, there is an inherent tension between calling upon Parliament to enact legal changes whilst simultaneously constructively challenging political parties. In the concluding section of this report we explore opportunities for addressing these tensions, and answering the legal and ethical questions posed by canvassing apps.

2 TECHNICAL ANALYSIS OF 2024 ELECTION CANVASSING APPS

To explore how data is used and shared by political parties' canvassing apps, we conducted technical investigations to analyse the infrastructure they are built upon. In particular we sought to answer two overarching questions:

- **How are the apps pre-configured to perform network requests to third party servers and other infrastructure?**
- **Do the apps have obvious backdoors that could allow unintended users to access their systems?**

We used a Static Application Security Testing (SAST) approach to explore these questions and canvassing apps' data flows. This involves looking at different aspects of the app's data collection to see how it is compiled and programmed to operate. This technique is often employed by security testers because it means the structure of an app can be tested in a sandboxed environment and free of threat of malware (though we were not expecting to find malware within apps). We also conducted some limited Dynamic Analysis Security Tests (DAST) of the apps whilst they were in live use – but only the apps functioning on log-in pages, as we did not attempt to secure log-in details provided to respective party members. As a result we performed a partial analysis of apps, with the possible insights and limitations outlined in Table 1.

4 Source: https://www.theguardian.com/politics/2024/apr/04/tories-planned-to-make-millions-from-members-data-with-true-blue-app

POSSIBLE SAST INSIGHTS	LIMITATIONS OF SAST ANALYSIS
· Can identify potential privacy violations by analysing the application's source code, byte code, or application binaries. · Can detect issues that may not be visible during runtime, such as hard-coded credentials or insecure data storage. · Provides a comprehensive view of the application's structure and potential security weaknesses.	· Cannot identify privacy violations that occur during the apps' operation after user log-ins, such as data leakage through network requests. · May produce false positives and negatives, depending on the complexity of the app. · Cannot identify issues that result from user interactions with apps, for example intentional or unintentional by-passing of security features.

Table 1: Summary of our investigative insights and limitations

We analysed canvassing apps used by three political parties: the Conservative, Labour and Liberal Democrat parties. With the exception of the web-based Labour Doorstep app, all of them were accessed via the Google Play Store. To facilitate the analysis we used a range of resources and tools including:

- APK Pure,[5] a website where users can download readable "Android Application Package" (APK) files[6] of various apps, files and games that run on Android devices. Many apps on the platforms have various version histories, which facilitates security audits.
- Mirror sites, which are websites or platforms that host copies (mirrors) of APK files for Android apps. These mirror sites are not official app stores like the Google Play Store, but provide APK files for a wide range of free and paid apps.
- Exodus Privacy – a privacy auditing platform for Android applications that can analyse APK app files (for example those accessed through APK Pure or mirror sites). It is able to identify in-built trackers (third-party components that collect information about the user and their actions), and analyse the permissions an app requests.
- The mobile security framework (MobSF) Static Analyser.[7] MobSF is a platform for conducting security research on applications, including penetration testing, malware analysis, and privacy analysis. For static analysis, MobSF conducts source code, binary, and configuration analyses on apps and generates automated reports on any vulnerabilities and issues uncovered.
- Charles Proxy,[8] a debugging tool that can be used for mobile app testing. It monitors the mobile traffic between an app and other parts of the internet whilst the app is running – including requests made to other servers and details of HTTP headers.

5 Link: https://apkpure.com/

6 An APK (Android Application Package) is the file format used to distribute and install applications on Android devices. It is essentially an archive file that contains all the necessary components of an Android app, including the app's code, resources, manifest file, and a digital signature.To inspect an APK for privacy violations, you would typically use tools or services designed for APK analysis. These tools can decompile the app, examine its code, and assess its behaviour, including data collection and communication with external servers.

7 Link: https://mobsf.live/

8 Link: https:// charlesproxy.com

The legitimacy of our analysis was contingent on sourcing APKs and app versions that were the same, or at least very similar, to those used by political parties during the election. To verify that the app versions we studied were authentic, we (wherever possible) validated the cryptographic signatures and hash values against those provided by the original app developers. For the web-based apps used by labour (that we could therefore not access APKs or app file details for) we relied primarily on Charles Proxy, and looked for public information[9] about IP addresses related to these apps.

Lastly, where this information was publicly available, we also reviewed apps' user manuals and parties' privacy policies to understand app functionalities, user modes, and potential data use.

2.1 ANALYSIS OF THE CONSERVATIVE PARTY'S VOTESOURCE CANVASSER APP

The VoteSource Canvasser app was used by the Conservatives to support canvassers with efficient data entry, helping them to *"spend more time talking to people and less time entering data"*.[10] It enables real-time data entry and syncing through canvassers' phones, and allows users to access campaign stats and search the associated database for constituent details.

In our investigation, we conducted a static analysis on several VoteSource Canvasser app versions[11] using MobSF on 12 September 2023. Through this, we identified the data trackers, urls, and software development kits (SDK) the app is associated with. An SDK is a set of external tools (compiled in one installable package) that provide app functionalities, and allow the app to be integrated with other external programs. Figure 1 shows where these app integrations and connections were present. Overall, the tracking software and SDKs in place for the app were in common use and likely to be seen as uncontroversial – for example using Microsoft Visual Studio App Center Analytics to send app analytics data to Microsoft.

Alongside the static analysis, we also ran a limited dynamic analysis on the aspects of the app that did not require a user login. Version 5.2.7 of the app was loaded in Charles Proxy in order to observe the requests it made. This analysis provided limited insights (in part due to technical issues encountered with the Charles Proxy analysis) but did at least validate the apps' connection with third party services identified in the SAST analysis.

9 Public information, or information in the public domain, is often called "open source", especially by policing and intelligence agencies, see for instance https://en.wikipedia.org/wiki/Open-source_intelligence and https://www.ibm.com/topics/osint however we avoid that term here as "open source" also means copyrighted material released under a permissive licence, intended for reuse and redistribution. See https://opensource.org/osd

10 Source: https://play.google.com/store/apps/details?id=com.conservatives.votesource&hl=en_GB&pli=1

11 Versions analysed included VoteSource 2.0.0.0, 1.3.2.0, 3.5.0.0,4.0.0.0, 4.0.0.1, 4.0.0.2, 4.1.0.1, 4.2.0.0, 4.3.0.0, 4.5.0, 4.6.0, 5.0.0, 5.1.1, 5.2.7

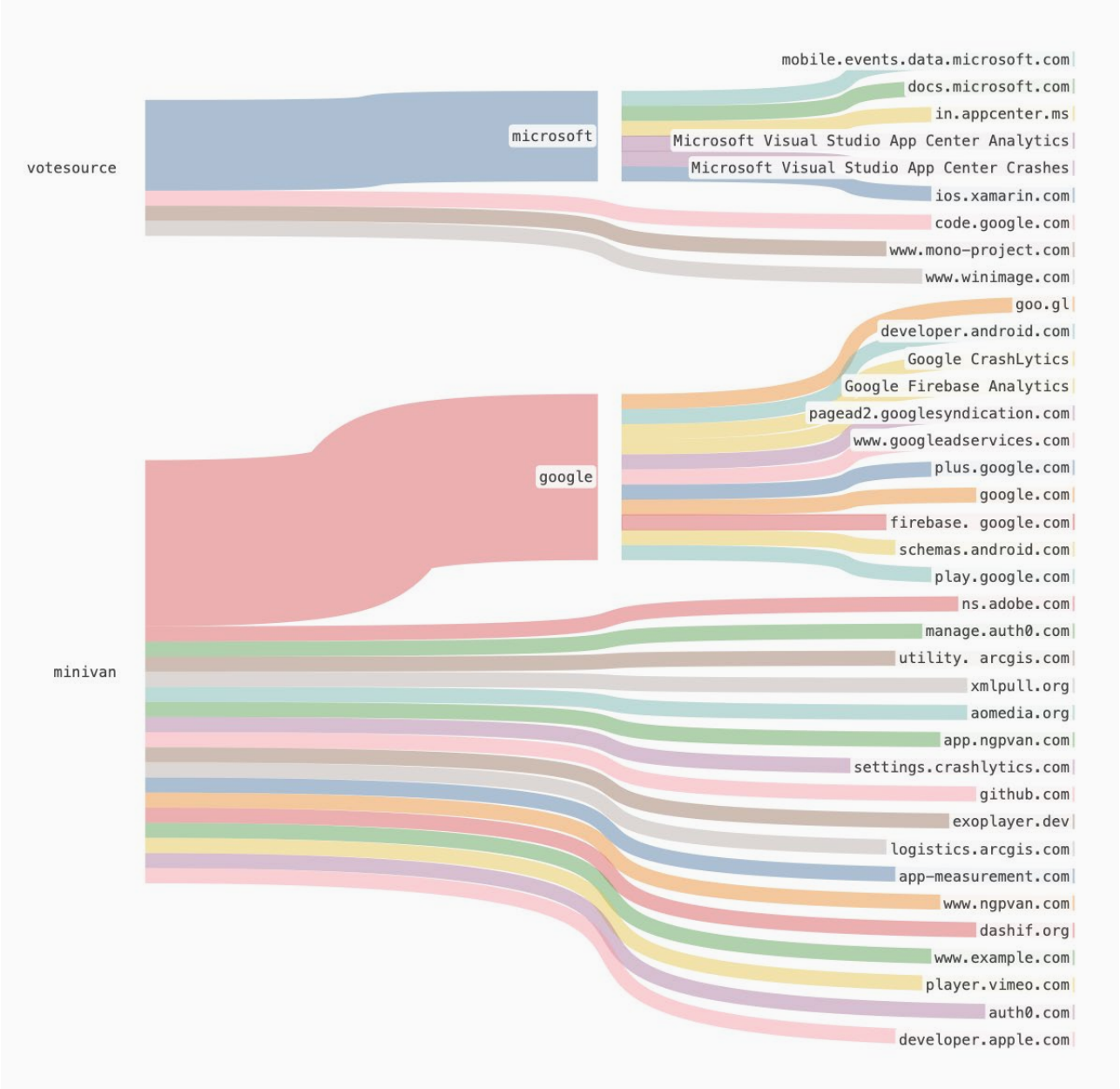

Figure 1: summary of third party URLs and SDKs the VoteSource app connected to.

A second application, called Share2Win was also used during the election. The Conservatives' Share2Win app was concerning. The security framework analysis tool alerted it to have stored secret credentials in both the Android and iOS versions potentially making it vulnerable to breaches (although this would need to be confirmed by the app developers), and various versions of it suffered from a number of further potential security issues, including "dependency confusion", where external libraries can be tampered with by a third party; missing privacy controls such as attributes for sensitive personal data (Android) and privacy manifest files (iOS). The Android app was able to access Wifi information which could lead to location tracking and strong identification of the user and their device.

Applications produced for political parties have to abide by data protection requirements, just as any other product or service. Our investigation called into question whether the legislation around data minimization, integrity, and confidentiality (article 5); Data protection by design and by default (article 25) and Security of processing (article 32) were being abided by.

We contacted the vendors about these issues, who stated that:

- the application versions you have tested are old versions which are no longer available on the Google Play Store or Apple App Store.
- The items outlined in your email are therefore all items that have either been resolved or have been internally investigated and closed with proper justifications by our security team. Any users who have auto-updates turned on in their mobile devices for the application will automatically get the new version of the app.

The app versions which were tested were in use during the election period, when the data was collected, and would be the versions downloaded by canvassers.

That appears to confirm that the issues were present during the election period, when the app was in greatest use.

The Share2Win application attracted media attention in the election when MPs personal information was breached.[12] The Telegraph reported that:

"Just by signing up to the app, launched in April, users could see the name, postcode and phone number of all 2,398 registrants in the space of a few clicks."

This involved basic inspection of the javascript of the "leaderboard" which was used to display which users had shared the most political content, through using the Developer tools in a browser like Chrome to view the source code. Using this capability did not require technical ability other than the ability to follow some simple instructions. This was downplayed by the Conservative party at the time, who however rectified the issue swiftly.[13] This is not the first time the Conservatives have had these kinds of problems; in September 2018, their party conference app revealed personal details including the phone numbers and addresses of many MPs attending.[14]

The Conservatives worked with Sprinklr to deliver the app. Sprinklr is a US-based marketing tech company, who have undergone a series of acquisitions to build up their capabilities.[15] This could cause problems with ensuring security in their product development. The company claims to to use AI to match individuals' identities in order to target and profile them. Their core data matching technology capabilities would likely be unlawful in the UK.

12 https://www.telegraph.co.uk/news/2024/06/22/conservative-leak-home-addresses-revealed/

13 "We believe only limited registration data was visible to authenticated users who would need to have technical competencies to actively search for a user and access that data, using specific developer tools."

14 https://www.bbc.co.uk/news/uk-politics-45693143

15 See appendix

2.2 ANALYSIS OF THE LIBERAL DEMOCRAT PARTY'S MINIVAN APP

MiniVan[16] was used by the Liberal Democrats for canvassing data collection, and is integrated with the Party's Connect database.[17] The app allows campaigners to access voter information and canvas lists, record doorstop responses, and update the Connect database in real-time.[18] It is built upon the NGP VAN platform – an American voter database and web hosting service provider used by various political parties (including a range of Democratic party presidential campaigns in America).

To analyse MiniVan, we loaded a series of available versions[19] into MobSF on 12 September 2023. We paid particular attention to in-built trackers, URLs and SDKs the app connected to, and other details relating to geolocation and IP addresses. Figure 2 shows the third party services and URLs the apps connected to. Where we observed discrepancies between different app versions, we investigated any that had potential privacy implications. We also conducted a Preliminary DAST analysis on the app using Charles Proxy on 12 September 2023, in order to verify that the findings identified in the SAST were valid.

From these analyses, a number of important insights emerged. MiniVAN version 9.2.0 (the most recent studied) uses Google Firebase SDKs (specifically one located at https://ngpvan-mobile-maps.firebaseio.com). Whilst this is not inherently problematic, it does point to potential security issues:

In March 2024, security researchers found that at least 900 websites built with Firebase were misconfigured, meaning an estimated 125 million user records (including phone numbers, emails, and bank details) were accessible.[20] This followed research by Comparitech in 2020 that found over 24,000 Android apps leaked data for similar reasons.[21] Elsewhere, security researchers have evidenced the various ways users can gain access to Firebase databases through front-end applications.[22] Commenting on this track record, A former Google software engineer recently stated that "concerns with security rules have always plagued [Firebase]".[23] Further DAST, conducted on the app after a user has logged-in, could potentially unpick how Google has access to the data gathered through the app through Firebase SDKs.

Given both the prevalence and recency (discovered just over a month before the UK election) of the Firebase misconfiguration security vulnerability, our findings relating to the security of MiniVan 9.2.0 are concerning[24] In other words, this vulnerability allows malicious third-parties to whom a decryption key was not shared with to decipher encrypted data. Therefore, while the app does use encryption, it may not be completely secure.

16 Source: https://tech.libdems.org.uk/training/connect/toolkit/using-minivan

17 Source: https://www.markpack.org.uk/136630/lib-dem-connect-login/

18 Source: https://d3n8a8pro7vhmx.cloudfront.net/libdems/pages/3956/attachments/original/1533743997/4.3_MiniVAN.pdf

19 App versions analysed include 9.1.0, 9.1.3, 9.1.1, 9.1.2, 9.1.4, 9.1.5, 9.1.6, 9.1.7 and 9.2.0

20 Source: https://blog.gitguardian.com/misconfigurations-in-google-firebase-lead-to-over-19-8-million-leaked-secrets/

21 Source: https://www.comparitech.com/blog/information-security/firebase-misconfiguration-report/

22 Source: https://www.sans.org/white-papers/39885/

23 Source: https://www.theregister.com/2024/03/18/google_firebase_cloud_security/

24 For example, the app used the encryption mode CBC with PKCS5/PKCS7 padding, which has been found to be vulnerable to padding "oracle" attacks. Source: https://github.com/mogol/flutter_secure_storage/issues/584

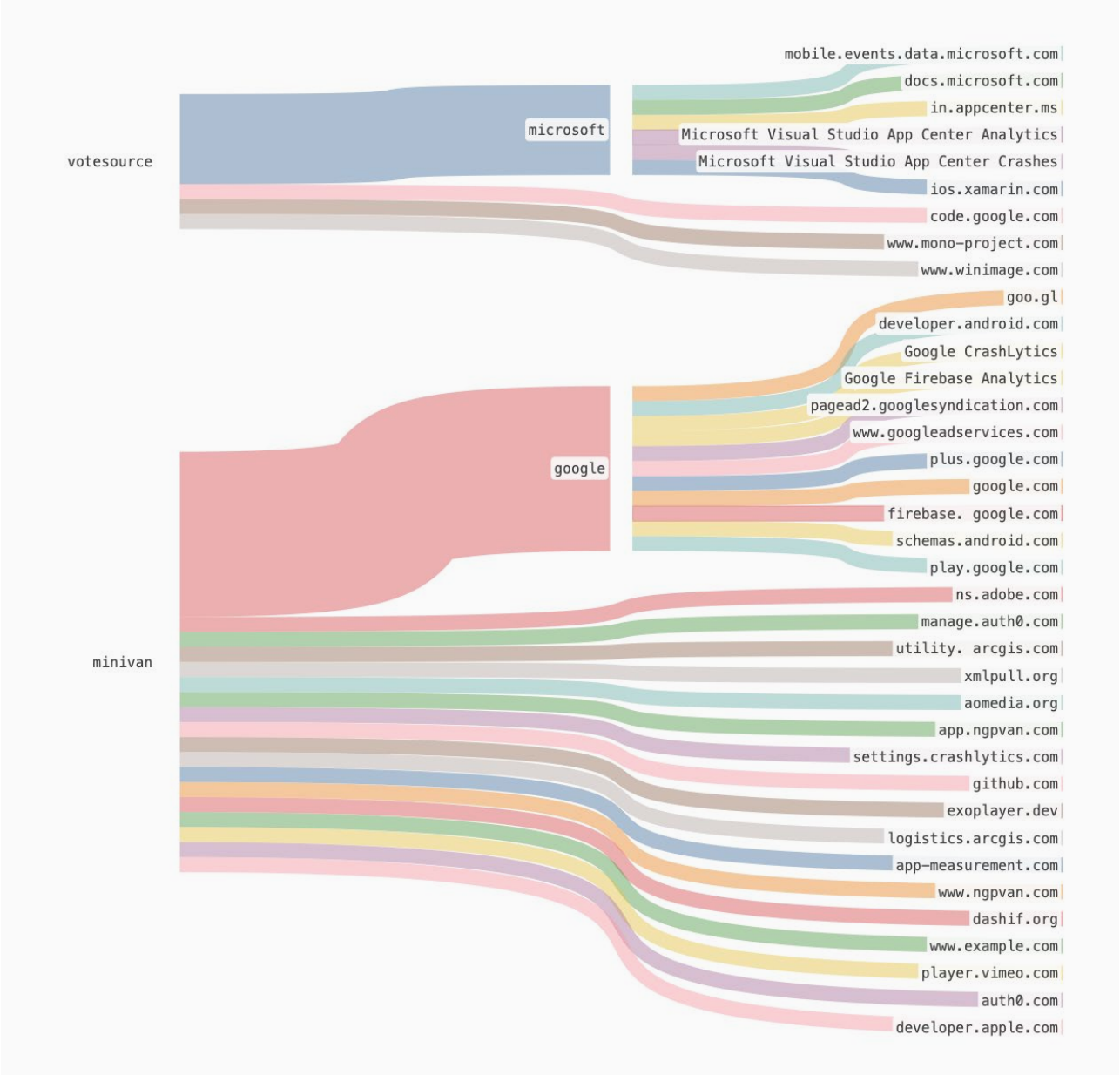

Figure 2: summary of third party URLs and SDKs the MiniVan app connected to (across all versions).

2.3 ANALYSIS OF THE LABOUR PARTY'S WEB-BASED CANVASSING APPS

Labour's canvassing operations for the 2024 election included three web-based apps – Doorstep,[25] Reach,[26] and Contact Creator.[27] Doorstep is used by UK Labour for canvassing and organising political campaigns. The app allows party volunteers, activists, and campaign organisers to access information about voters, and helps with targeting specific individuals for canvassing efforts (for example by providing information on voter preferences). Users can also input data from their interactions with voters, helping the party to deepen its understanding of voters. Contact Creator is the party's online

25 Source: https://doorstep.labour.org.uk/

26 Source: https://reach.labour.org.uk/

27 Source: https://labour.org.uk/wp-content/uploads/2022/10/AC2022-Using-Contact-Creator-to-run-reports-and-enter-data.pdf

voter database. Its users are set-up with one of three account types depending on their role in campaigns: "Data Entry" accounts can only enter data, or search for individuals within their database or the Marked Electoral Register (which shows who has or hasn't voted in the previous election). "Standard" accounts can also run reports and statistical calculations on these databases, while "Local Admin" users from Constituency Labour Party groups have the power to create user accounts.

Given Doorstep, Reach and Contract Creator were unavailable in mobile app form, we took an alternative approach to the one used to analyse MiniVan and VoteSource Canvasser (that primarily used MobSF). Here we used Charles proxy to record network requests after loading the web-based services, and looked for relevant public information about associated IP addresses. We used Censys Search[28] – a service providing searchable datasets that provides insights on the relevant for security investigationson the internet. Most pertinently for our analysis, this includes details on who hosts websites and IP addresses.

The DNS records (that translate user-friendly domain names into IP addresses so that web browsers can load associated Internet resources) associated with Doorstep suggests it is run using Amazon servers. A partial DAST analysis of Doorstep did not reveal any suspicious behaviour. Each of the API calls we observed were associated with essential components for the app, and verified the identity of the user of the app in a way that at face value appears largely secure and compliant. Analysing Labour's canvassing web-apps on Censys Search did however yield some interesting findings:

- **An Autonomous System (AS) is a connected group of IP addresses (and associated website domains) managed by a single organisation. A search for the Doorstop's address – *reach.labour.org.uk* – found that it was part of an AS belonging to Experian UK.[29]**

- **We found confirmation that Contact Creator is also associated with Experian's infrastructure, as clearly shown by the URL address provided in Labour's Contact Creator training manual:[30] https: trn.contactcreator.uk.experian.com/touchpoint**

- **Analysing historical DNS records on Security Trails[31], we found that records for Labour's Contact Creator (trn.contactcreator.uk.experian.com) have been visible since 27 October 2018. Data for *Reach* show DNS records dating back to 18 July 2020 – this could indicate the date of implementation, but only the app developers or political party staff could confirm this.**

Overall, it is clear that Experian has played a role in hosting or developing key parts of Labour's canvassing infrastructure. In the absence of a more holistic investigation involving DSAT (likely requiring the ability to log on to their web-based canvassing apps) how data is shared between Labour and Experian is less obvious. Labour's General Electorate privacy policy does not provide much further clarity – it explains that the party's "indirect data collection" includes *"Demographic data about you from our commercial supplier (Experian)"*, but does not provide further explicit detail on what this data is or how it is used.

28 Link: https://censys.com/

29 A Censys search for details relating to *reach.labour.org.uk* on 12 September 2023 yielded:
"Basic Information
Network EXPERIAN-AS (GB)
Routing 194.60.160.0/19 via AS33953
Protocols 443/HTTP"

30 Source: https://labour.org.uk/wp-content/uploads/2019/10/Contact-Creator-Selections.pdf

31 Source: https://securitytrails.com/

3 ADDRESSING THE UNANSWERED QUESTIONS AROUND CANVASSING DATA

3.1 HOW CAN POLITICAL PARTIES BE MORE TRANSPARENT AROUND THEIR USE OF CANVASSING APP DATA?

The findings of our analysis do not provide definitive evidence or the suggestion that the parties have broken data protection law or acted unethically – they instead point to potential issues with wider implications, which can go unremediated when not given time or attention. Parties' privacy policies and other relevant documentation could go someway to reassuring the public around these issues, but are too generic and vague to do so. Table 2 summarises what information is provided by the Labour, Conservative and Liberal Democrat parties on canvassing app data governance. Cross-referencing these data policies against our analysis, and comparing policies against each other, suggests several issues relating to transparency and trust:

- **All parties rely on generic privacy policies to explain how canvassing data is governed. To be more transparent, parties could publish copies of consent forms and privacy policies provided to those being canvassed that provide more granular detail on how data is used.**
- **Policies state or imply that voters are sometimes being targeted for canvassing due to data profiling that identifies them as receptive to parties' messaging. Voters should be made aware that this is the case at the point they are door-stopped, if this information is not already provided in consent forms.**
- **Parties could do more to be transparent about the organisations canvassing data is shared with. The Conservative party does not explicitly name the third parties it shares canvassing data with in their privacy policy, whilst the Liberal Democrats seemingly does not mention its canvassing data-sharing with Google (which was suggested by our analysis).**

The contestation of the 2020 US election results, and the role disinformation networks played in accelerating the July 2024 riots in the UK, illustrate the present fragility of trust in Western democratic systems. In this context, a proactive approach to transparency and trust-building by political parties seems particularly important. This should extend to how election campaigns, and the data infrastructure underpinning them are delivered.

RECOMMENDATIONS

- **Political parties must urgently publish in the full list of organisations they share canvassing data with.** Our research suggests some parties only refer to generic organisation types (e.g. "commercial partners"), whilst others do not appear to have listed the organisations our technical analysis suggests are involved in supporting canvassing apps.
- **Political parties should collectively agree to publish financial details of agreements with commercial providers to provide canvassing infrastructure.** This would help to highlight any deals where data assets implicitly form part of the value of a commercial agreement (for example where data brokers provide free access to infrastructure in exchange for data access).
- **Political parties should proactively publicly publish canvassing data protection policies to maintain trust** – for example publishing DPIAs for canvassing apps, specific data sharing agreements with third parties, and privacy consent forms provided to voters. Our research team could find no public evidence of such materials, beyond general privacy policies and some partial information within app user manuals.

	LABOUR'S POLICY	CONSERVATIVES' POLICY	LIBERAL DEMOCRATS' POLICY
Canvassing app data processing	We could find no public information on privacy policies specifically related to Labour's web-based canvassing apps (user support documentation found did not explicitly address privacy). Labour separates its privacy policies based on types of stakeholders (e.g. volunteers and members) and processing.[32] Its "General Electorate Privacy Notice" was last updated on 5 March 2024. It highlights that they obtain personal data "on the doorstop", and describes how face-to-face canvassing data is processed under *"GDPR Article 6.1(e), also known as "Public Task". And, Special categories of personal data used for the purpose of Substantial Public Interest under UK GDPR Article 9.2(g)"*. A separate Profiling policy[33] outlines how data is used "to make predictions about individual electors, wide demographic groups or areas of the country".	We could find no public information on privacy policies specifically related to the VoteSource App. Section 4.1 of the party's general privacy policy[34] explicitly explains how the party uses data on "canvassing political opinions", and also helpful provides specific details on data used for *"Providing our VoteSource Canvasser Application for doorstep data collection"*. The data potentially gathered for this task is extensive, and includes *"Name, Address, Electoral Roll Number, Polling District, Political Opinion, Voting History, Contact Details (email, phone, social media etc), Survey Responses, Membership History, Telling and Knocking Up Information, Username, Hashed Password, IP Address, Geolocation, Device information, Usage data and history"*. They rely on two legal bases for this processing – Public Task and Legitimate interests. Section 5 of the policy highlights how data from canvassing contributes to profiling of the electorate that *"provide [the party] with competitive insight into the political landscape and general trends, and to allow us to better understand the electorate as a whole"*.	The MiniVan training content contains a short section on GDPR compliance.[35] This advises canvassers to get public consent as part of a survey citizens are asked to fill out, after providing them with a leaflet containing information about LibDems privacy policy. Screenshots accompanying the guidance imply that the policy in question is the party's general Privacy and Cookie Notice.[36] This policy was last updated prior to the election on 14 December 2023. This policy makes mention of canvassing in the context of a section explaining how data is used for political campaigning – including that they rely on *"UK GDPR Article 6(e): Public task, Article 9(2)(g) Substantial Public Interest and DPA 2018, Schedule 1, Part 2, Paragraph 22 (1)"* as their legal basis for processing and that they retain data for 3 election cycles. The policy also states that they *"may also analyse and make predictions on the data we hold about [the public]"*, and links to a separate data profiling policy[37] to explain how. In that policy, canvassing is explicitly mentioned as a potential data source for a range of profiling activities. This profiling, in the party's view, "is to engage with voters and encourage democratic engagement" and carried out under a legitimate interests legal basis. One use case relevant to canvassing is the use of profiling to *"Decide which addresses we will send our volunteers to, in order to improve the chances of them having enjoyable and productive conversations"*.

Table 2: Summary of political parties' public information on canvassing data policies

32 Link: https://labour.org.uk/privacy/privacy-notices/

33 Link: https://labour.org.uk/privacy/privacy-notices/profiling-privacy-notice/

34 Link: https://www.conservatives.com/privacy

35 Source: https://tech.libdems.org.uk/training/connect/toolkit/using-minivan

36 Link: https://www.libdems.org.uk/privacy

37 Link: https://www.libdems.org.uk/privacy/data-profiling

	LABOUR'S POLICY	CONSERVATIVES' POLICY	LIBERAL DEMOCRATS' POLICY
Third party data sharing	Labour's privacy policy explicitly states that they obtain data from *"our commercial supplier (Experian), and BT Osis (indirect data collection)"*. The latter is a telephone directory operated by BT. Their policy states that the party never sells personal data, and that each third party data recipient is *"subject to review by the Data Protection Team to make sure they have the right methods in place for keeping your personal data secure"*. The policy does not identify which specific parties data is shared with, and only uses generic categories such as "An electoral roll database management service provider". Commercial data brokers are not mentioned. The party's profiling policy explains how their profiling activity includes purchasing demographic data from their "commercial suppliers", and sharing data with *"1. Pre-approved digital profiling system providers;* *2. Pre-approved online survey or questionnaire platform providers;* *3. Pre-approved digital communications and storage providers; and* *4. Pre-approved expert social media platform analysis and maintenance providers."* It does not state who these pre-approved providers are.	Section 8 of the party's general privacy policy explains who they share personal data with. The content is relatively generic: it states that data will never be sold, but only provides a list of types of third parties data could be shared with (without identifying specific organisations and details on specific processing). Of the types of third parties identified, "data analytics companies" is one category.	The Liberal Democrat's profiling policy provides a contact address for opting out of this processing, but does not provide any details on if or how third parties are involved. Their general privacy policy does however clearly state that *"The Party will not sell [public] personal data to third parties"*. The party's "Who we share data with" policy,[38] last updated on 5 June 2024, outlines which external providers they share data with and when. Data relating to "political opinions from canvassing" is shared with Connect / NGP Van and EARS – an electoral register database. There is no explicit mention of sharing data with Google Firebase for canvassing app services or analytics (although it does mention the use of Google Analytics for website visitors).

Table 2: Summary of political parties' public information on canvassing data policies

38 Link: https://www.libdems.org.uk/privacy/data-sharing

3.2 ARE POLITICAL PARTIES OVER-RELIANT ON COMMERCIAL CANVASSING APP INFRASTRUCTURE?

The Conservative, Liberal Democrat and Labour parties are, to differing degrees, increasingly reliant on commercial entities to run their digital campaigning infrastructure. There are many legitimate potential reasons for this – the pace of elections necessitating the quick purchase of off-the-shelf solutions, challenges in building sophisticated in-house digital teams, and fears of the electoral costs of building inadequate systems likely among them.

The commercial space for canvassing apps is a microcosm of the wider digital economy, where a small number of data brokers and multinational tech companies own a substantial share of the market. In Labour's case Experian – one of the "Big Three" global credit agencies – provides the party with database resources. The Conservative and Liberal Democrat apps are built upon app infrastructure provided by Google and NGP VAN respectively. The latter is a subsidiary of Bonterra (formerly EveryAction, Inc) which was acquired by global private equity firm Apax Partners in 2021.

The size of these organisations means there is a power asymmetry between them and political parties – potentially making it harder for parties to assert control over how apps are designed and governed. Where companies are headquartered outside of the UK – as is the case for Alphabet and Experian – this may create practical challenges for the ICO where they have to pursue extraterritorial investigations.[39] The security challenges associated with Google Firebase (discussed in section 2.2 in the context of Liberal Democrats' MiniVan app) are also emblematic of a wider trend. Here, systemically important technology companies, and the infrastructure they run, are more commonly targeted by hackers due to the size of potential rewards.[40]

RECOMMENDATIONS

- The ICO and Electoral Commission must develop new "anticipatory" regulatory assurance programmes that ensure political campaigning is lawful before and during elections – not retrospectively after they have concluded and damage is already done. This could include the ICO delivering a regulatory sandbox scheme or committing to proactive assurance audits for all major political parties' canvassing apps.
- The current Labour government should introduce new measures to strengthen governance of political canvassing and opinion data under the DUA Bill and election reform agenda. This will deliver on their commitment in the King's Speech to "strengthen the integrity of elections". Reforms should include mandatory public publication of political opinion data sharing agreements, and outlawing the use of canvassing data for commercial benefit.
- The Data Use and Access Bill should be amended so that a future Secretary of State cannot legalise wider use of data for electoral purposes through Henry VIII powers.

39 Source: https://uk.practicallaw.thomsonreuters.com/w-041-5162?transitionType=Default&contextData=(sc.Default)&firstPage=true

40 Source: https://aisel.aisnet.org/cais/vol52/iss1/12/

3.3 ARE RELATIONSHIPS BETWEEN POLITICAL PARTIES, DATA BROKERS, AND APP SERVICE PROVIDERS LAWFUL AND ETHICAL?

Of the insights uncovered by our analysis, perhaps the most troubling is the British political system's enduring relationship with Experian. ORG's previous research has explored the legal and ethical issues posed by many parties' – including Conservative, Unionist, and Labour – purchasing of Experian's political profiling datasets.[41]

In this instance the party concerned is Labour; our findings invite the question of whether the data broker accessed the party's canvassing data to develop its own datasets. Experian could well be one of the *"pre-approved digital profiling system providers"* Labour mentions within its privacy policy. If true, this could challenge a range of core UK data protection laws principles including:

- **Transparency,** if individuals are not adequately informed that it will be shared with Experian.
- **Fairness,** if data use has an adverse impact on data subjects or people were deceived to obtain it (for example if they believed it would solely be used by political parties).
- **Purpose limitation,** if data obtained for the purpose of democratic engagement is then further used to commercially benefit Experian.

Furthermore, data related to political opinions is defined as special category data under the UK GDPR. Some other sensitive forms of data that could be revealed during doorstop conversations (including relating to religious beliefs, race or union membership) also falls under this definition. The sensitivity of such data means it warrants significant additional protection under law, and it can only be processed if the organisation doing so can identify a suitable legal basis for doing so under Article 9 of UK GDPR.[42] Political parties typically rely on condition (g), *Reasons of substantial public interests (with a basis in law)*, with that "basis in law" being democratic engagement under the Data Protection Act 2018.

The ICO's guidance on political campaigning states that *"[the reasons of substantial public interests] lawful basis is often misunderstood as an overarching exemption, so it is important that you understand the purpose of the provision."*[43] In short, canvassing data for political parties to use to promote democratic engagement is in the public interest, sharing it with data brokers for commercial benefit is certainly not. In this context, any Experian processing of political opinion data is only likely to be lawful with explicit consent on the data subjects. The ICO has also stated that it considers data matching – combining, comparing or matching personal data obtained from multiple sources – as high risk.[44] Political parties, and third party data providers, should therefore take steps to manage these risks such as publishing Data Protection Impact Assessments.

In the absence of consent it is possible that Experian and other data brokers could aim to anonymise data, thereby exempting itself from the UK GDPR. Even assuming that this is done lawfully (by genuinely anonymising, not

41 Source: https://www.openrightsgroup.org/app/uploads/2020/07/200619%E2%80%94org%E2%80%94report.pdf

42 These conditions include (a) Explicit consent (b) Employment, social security and social protection (if authorised by law) (c) Vital interests (d) Not-for-profit bodies (e) Made public by the data subject (f) Legal claims or judicial acts (g) Reasons of substantial public interest (with a basis in law) (h) Health or social care (with a basis in law) (i) Public health (with a basis in law) (j) Archiving, research and statistics (with a basis in law). If organisations rely on conditions (b), (h), (i) or (j), they also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018. Source: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data/#:~:text=drawing%20that%20inference.-,What%20are%20the%20rules%20for%20special%20category%20data%3F,Article%206%20basis%20for%20processing.

43 Source: https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1/lawful-bases/#publictask

44 Source: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

pseudonymising, data), widespread harvesting of voter data for commercial benefit via canvassing is still ethically dubious. This is a particular concern given the wider potential conflicts of interest at play in this space: As of 6 October 2024 11 members of the House of Lords have a registered interest in Experian,[45] whilst Apax partners invest in a range of technology and internet services that could benefit from consumer data being shared between them.

RECOMMENDATIONS

- The ICO investigates if and how data has been shared between Labour and Experian throughout the 2024 election period. This is critical given the various potential data protection compliance issues and risks raised by our investigation, and the history of regulatory activity focused on Experian and political campaigning.
- The ICO should provide explicit guidance that sharing of election canvassing data with third parties constitutes "large-scale" processing of special category data – meaning it is high risk processing under the UK GDPR, and heightened safeguards and DPIAs are required. This should remain the case even where data is pseudonymised.
- The government's proposed Integrity and Ethics Commission should investigate the relationships between data brokers and elected officials as a priority – recognising that transfer of data to third parties is essentially transfer of money given the significant value of these datasets, and should therefore be held to the same public standards and levels of scrutiny as financial interests.

APPENDIX I

Sprinklr is a marketing and advertising technology business:

Sprinklr connects to "25 social platforms" and "millions of blogs, news sites, review sites, forums," and messaging platforms. It gathers data from "3.4 billion active social media users" and "60 billion messages sent per day."

Their US platform uses an AI-powered data flow engine that claims to process "unstructured customer conversations" into seven layers of listening. This includes "sentiment, emotion & spam identification," "language detection & entity extraction," "image insights," "verticalization insights," "audience insights," "location insights," and "rules & alerting."

Sprinklr's US services include a data conversion engine which translates unstructured data into structured data. This involves tagging data with "message ID," "audience profile ID," "business location ID," and "product ID." The platform converts unstructured data into "structured experiential data" and "structured operational data." This provides a "360-degree view" of the customer, enabling businesses to gain insights into customer behaviors and preferences.[46]

Sprinklr uses its venture capital funding to "acquire smaller firms that have the tools Sprinklr wants to build itself", then "discards the purchased technology" and has the acquired company's employees "develop a native Sprinklr version of the software".[47]

45 Source: https://members.parliament.uk/members/lords/interests/register-of-lords-interests?SearchTerm=experian+&ShowAmendments=False

46 Screenshots from 'How Sprinklr Works' accessed via Youtube https://www.youtube.com/watch?v=qWkDDB4HFLE

47 https://www.forbes.com/sites/alexkonrad/2016/01/20/meet-sprinklr-the-startup-that-cracked-social/#4b6a9cc1a23e

Recent acquisitions:

March 2014: Sprinklr acquired Dachis Group.[4849]

August 2014: Sprinklr acquired TBG Digital.[50]

September 2014: Sprinklr acquired Branderati, 'a word-of-mouth advocacy marketing company'.[51]

February 2015: Sprinklr acquires Pluck, for 'managing the complete social customer journey'.[52]

April 2015: Sprinklr acquired Get Satisfaction.[53]

April 2015: Sprinklr acquires Scup, 'a leader in social media monitoring, customer care, and analytics technology'.

June 2015: Sprinklr acquired NewBrand, a 'location-specific text analytics software company'[54]

November 2015: Sprinklr acquired Booshaka, 'an advanced audience segmentation and management platform'[55]

April 2016: Sprinklr acquired Postano, 'the world's leading social data visualization platform'. [56]

November 2016: Sprinklr acquired Little Bird.[57]

December 2019: Sprinklr acquired Nanigans' social advertising business.[58]

Statement from Sprinklr

As we are sure you will appreciate, we have legal and contractual obligations to our clients relating to confidentiality, and we cannot discuss specific client configurations or alleged security matters related to those clients externally.

With respect to the information included in your message, the application versions you have tested are old versions which are no longer available on the Google Play Store or Apple App Store. The items outlined in your email are therefore all items that have either been resolved or have been internally investigated and closed with proper justifications by our security team. Any users who have auto-updates turned on in their mobile devices for the application will automatically get the new version of the app.

Please note that Sprinklr takes reports of vulnerabilities extremely seriously and investigates all reported issues with internal teams. All issues received are investigated, triaged, assigned a criticality rating in accordance with industry-standard vulnerability management processes, and remediated accordingly. Sprinklr also actively monitors for such issues internally through annual penetration testing, which is conducted on our applications within a controlled environment. These annual application penetration tests deliver valuable insights into the potential vulnerabilities present in the production applications provided to our customers. Additionally, Sprinklr is regularly audited by third-party assessors to evaluate internal controls that protect the security, confidentiality, integrity, availability, and privacy of the information entrusted to us by our customers. Sprinklr is certified to SOC 1,2,3, PCI-DSS, ISO-27001, and FedRAMP LI-SaaS.

Maintaining the protection and security of our customers' data is always of paramount importance. Sprinklr engages in robust due diligence with our customers as it relates to data privacy and security and full details on Sprinklr's security and privacy program, including our third-party audits, can always be found at https://trust.sprinklr.com/.

---

48 https://www.crunchbase.com/organization/dachis-group

49 https://www.sprinklr.com/blog/sprinklr-acquires-dachis-group/

50 https://www.sprinklr.com/blog/sprinklr-acquires-tbg-digital-social-advertising/

51 https://www.crunchbase.com/organization/branderati

52 https://www.sprinklr.com/blog/sprinklr-acquires-pluck/

53 https://investors.sprinklr.com/news/press-releases/detail/47/sprinklr-acquires-leading-location-specific-text-analytics

54 https://investors.sprinklr.com/news/press-releases/detail/47/sprinklr-acquires-leading-location-specific-text-analytics

55 https://techcrunch.com/2015/11/02/sprinklr-acquires-booshaka/

56 https://investors.sprinklr.com/news/press-releases/detail/39/sprinklr-acquires-social-visualization-leader-postano

57 https://www.sprinklr.com/blog/sprinklr-acquires-little-bird-for-influencer-marketing/

58 https://www.sprinklr.com/newsroom/sprinklr-acquires-nanigans-social-advertising-business/

openrightsgroup.org

Published and promoted by Open Rights Group, a non-profit company limited by Guarantee, registered in England and Wales no. 05581537. Registered address Space4 113-115 Fonthill Road, London, England, N4 3HH