

# Personal Voter Data Use in the 2019 Ukrainian Parliamentary Elections: A Report on Digital Influence Outside the Scope of Disinformation

TETYANA BOHDANOVA  
2020 Fellow, Prague Civil Society Centre



July 2020

# Acknowledgements

This report has been prepared in cooperation with representatives of Ukrainian and international civil society organizations due to the generous support of the Prague Civil Society Centre. The views expressed in this report reflect the views of the author and contributors listed further and do not necessarily reflect the views of the Prague Civil Society Centre or any other organization.

Author: Tetyana Bohdanova, Spring 2020 Fellow, [Prague Civil Society Centre](#), Prague

Legal commentary: Vita Volodovska, Head of Legal, [Digital Security Lab](#), Ukraine

Facebook data analysis: Robert Lorian, Data Analyst, [Civil Network OPORA](#), Ukraine

Digital security review: Vadym Hudyma, Digital Security Specialist, [Digital Security Lab](#), Ukraine

General guidance: Varoon Bashykarla, Data Scientist, [Tactical Technology Collective](#), Berlin

# Table of Contents

|  |    |
|--|----|
| Table of Contents  | 3  |
| 1. Intro: research purpose, scope, and methodology   | 4  |
| 2. 2019 Election cycle: background and challenges  | 5  |
| 2.1. Disinformation, cyberattacks, and concerns about 2019 foreign election interference                                 | 5  |
| 2.2. The 2019 Presidential elections and the arrival of targeted online political speech                                 | 6  |
| 2.3. New Facebook regulations for elections  | 6  |
| 2.4. Parallel use of legitimate and questionable online campaigning practices in Presidential elections                  | 7  |
| 3. 2019 Parliamentary elections  | 7  |
| 3.1. Digital campaigning methods and practices: an overview  | 7  |
| 3.2. Facebook political advertising during Parliamentary elections   | 13 |
| 3.3. Other issues with digital campaigning   | 14 |
| 4. Online campaigning and data collection by five Parliamentary parties  | 14 |
| 4.1. Legal framework   | 14 |
| 4.2. Websites  | 16 |
| 4.2.1. Website security  | 27 |
| 4.3. Other methods of data collection during digital campaigning: Facebook, Google forms, mailing lists, petitions, etc. | 31 |
| 4.4. Messengers and chatbots   | 40 |
| 5. Other sources of citizens' personal data  | 41 |
| 5.1. State Voter Registry  | 42 |
| 5.2. Leaks, hacks, and security concerns   | 43 |
| 5.3. Semi-legal or illegal sources   | 43 |
| 5.4. Consumer data   | 46 |
| 5.5. Plausible sources of voter data in the 2019 political campaigning   | 46 |
| 6. Considerations of pre- and post-election data ownership and sharing   | 47 |
| 6.1. Party-affiliated projects   | 47 |
| 6.2. Government entities and elected representatives   | 48 |
| 7. Conclusions   | 50 |

# 1. Intro: research purpose, scope, and methodology

2016 was a significant year in the history of political campaigns, with the US Presidential elections, the UK's "Brexit" referendum, and consequent revelations sparking a worldwide discussion about the role of social media in elections and the significance of the use of personal voter data for digital campaigning. Ukraine had some time to take the lessons learned from these events into consideration and modernize its legislation regarding digital election campaigning ahead of the 2019 Presidential and Parliamentary votes, yet no changes to either existing or the newly adopted Electoral Code have been made to reflect the latest challenges posed by new technology.

While several civil society organizations have produced detailed reports about 2019's online political campaigning in Ukraine and its implications, no investigations have been made into the use of personal voter data in elections and the issues arising at the intersection of privacy and digital campaigning. **The purpose of the given report is to fill this gap by looking at the treatment of personal voter data by five parties elected to the Parliament during the course of 2019 electoral cycle: the Servant of the People (Слуга народу) party, the European Solidarity (Європейська солідарність) party, the Batkivshchyna (Батьківщина) union, the Opposition Platform — For Life (Опозиційна платформа — За життя) party, and the Holos (Голос) party.**

In particular, in this report we look at the online data collection practices used by these political parties during the 2019 Parliamentary campaign period on their official websites and social media accounts, including popular messenger platforms. We review these practices against the existing legal framework, the claims about how voters' personal data was being collected and processed by the parties themselves (i.e. in privacy policies on their websites), and the digital campaigning methods and tools utilized by political actors during the 2019 elections. We also attempt to put our findings into a wider context by providing background on the state of personal citizen data security and describing a few incidents of significance for understanding the current discourse around privacy issues in Ukraine. When investigating social media campaigning, we have particularly benefited from the data on Facebook activity and paid political advertising of parties and candidates [accumulated by the Civil Network OPORA](#) during the 2019-2020 period. Additionally, we use the information obtained from media publications, [reports of watchdog organizations](#), and interviews with persons possessing extensive background in election issues and digital political marketing in Ukraine.

At the same time, the scope of this report is limited by us conducting a largely external review of political parties' digital activity. For instance, we did not have access to any backend IT or CRM systems utilized by the parties during the elections; hence, we could not obtain a full grasp of their data collection and processing practices nor the data's usage in digital campaigning. Moreover, our overview of targeted digital campaigning and voter engagement practices is

largely limited to Facebook, due to it being a shared campaigning platform used by all five parties in question, its capabilities for running micro-targeted political ads, and the availability of granular data on voter engagement practices. In our review of parties' websites and social media activity, we focus on official websites (if a party operated more than one, we focus on the one mainly used for voter engagement and data collection during elections) and their official Facebook pages, with the exception of cases when affiliated pages ran paid political advertisements on a party's behalf. Additionally, in order to conduct a comprehensive review of parties' digital activity during elections, we at times look at the websites and social media accounts retrospectively with the use of an Internet archive. In addition, we do not provide a systematic review of regional, affiliated, or individual candidates' websites and their social media activity and only mention those where necessary for presenting a full picture of digital campaigning methods and treatment of voter data.

## 2. 2019 Election cycle: background and challenges

### 2.1. Disinformation, cyberattacks, and concerns about 2019 foreign election interference

There is ample evidence that Russian state actors and associates have targeted Ukraine with disinformation campaigns since at least 2014, with the Oxford Internet Institute once referring to attacks waged against the county as "[the most globally advanced case of computational propaganda](#)." For instance, in 2016, the Ukrainian internet portal Texty.org.ua uncovered a coordinated network of [more than 2,000 Facebook profiles](#) linked to a Russian troll farm, which for nearly eight months led an online campaign that sought to topple the Ukrainian government. A 2018 study by VoxUkraine analyzed over [nine million tweets linked to the IRA](#), of which 750,000 related to Ukraine. This disinformation campaign appears to have been sparked by the 2014 Euromaidan revolution and has steadily gained ground through the occupation and annexation of Crimea, peaking the day after Malaysian flight MH17 crashed in eastern Ukraine.

These and other instances have prompted concerns about the 2019 elections and the possibility of foreign interference. However, while Russian disinformation during the election period [remained as rampant as ever](#) and [Russia-linked hackers](#) attempted to disrupt state electronic infrastructure, these [were deemed not extensive enough](#) to affect the voting process or the electoral outcome.

## 2.2. The 2019 Presidential elections and the arrival of targeted online political speech

With [21.4 million internet users](#) and [23.5%](#) of Ukrainians turning to social media as their main source of news, 2019 was the first year when social networks made a significant [impact](#) on political campaigning. The trend was set by Volodymyr Zelenskyy, who managed to engage an audience not previously interested in elections yet active on Facebook, Instagram, and Telegram. He also imposed new “rules of the game” on his political opponents, including the incumbent President Petro Poroshenko, who extended his campaign from Facebook to both Instagram and Telegram.

According to Zelenskyy’s chief digital strategist — later Ukraine’s Minister of Digital Transformation Mykhailo Fedorov — the main focus of their campaign was user engagement, for which the headquarters created a number of special initiatives that offered voters various options for getting involved. Another special tactic of Zelenskyy was the extensive use of the micro-targeting functionality offered by digital platforms, in particular Facebook, for delivering tailored messages to different groups. To Fedorov’s [own admission](#), in the course of the election, the campaign segmented its audience into 32 categories according to age, gender, professional affiliation, or political interest and ran over 3,200 targeted advertising campaigns. It also sent [21 million](#) emails, amassed 130,000 subscribers on its Telegram channel, and recruited 608,527 volunteers online, including 20,000 election observers and 10,000 commissioners that provided detailed personal information in order to serve in such capacity. The team also launched a number of chat-bots, one of them helping voters find their polling places based on their place of residence.

## 2.3. New Facebook regulations for elections

Ahead of the 2019 Presidential elections, Facebook [announced](#) new regulations aimed at curbing misinformation and foreign interference by increasing transparency around paid political advertising and vowing to monitor user behavior more closely. The new rules require those placing political ads to [disclose their identity and location and provide a “paid for by” disclaimer](#) for Facebook’s approval. Facebook has also opened a public political advertisements library, containing all Ukraine-related political and social ads that ran with or without a disclaimer and have been determined to contain political or issue-based content.

Yet, the new transparency regulations did not come into effect until less than two weeks before the first round of voting, were slowly enforced, and left significant loopholes. For instance, one could get around the geographic requirements through “account rental” to an advertiser from abroad — a practice which the State Security Service [warned](#) about in January of 2019. Additionally, the problematic content reported by campaigns was [removed with a significant delay](#), and pages that repeatedly violated the rules were [still allowed](#) to attempt to buy ads.

Finally, it bears mentioning that similar transparency measures have not been introduced by other online platforms such as Twitter or Google, rendering political advertising on such platforms as YouTube virtually unaccountable to any authority.

## 2.4. Parallel use of legitimate and questionable online campaigning practices in Presidential elections

While monitoring paid political advertising on Facebook, Ukrainian election observer OPORA and international watchdog Democracy Reporting International uncovered [dodgy Facebook pages](#) with [links to official accounts](#) of main election contenders that spread misleading and compromising information about their opponents.

Additionally, election observers [noted](#) active usage of bots and fake accounts in the course of online campaigning that were often detected and removed by the platforms themselves. Investigative journalists managed to interview several persons that ran such accounts on commercial grounds. According to one interviewee's estimate, during the 2019 election season [over 200,000 such accounts](#) may have been active on Facebook alone, while a cost of one such "operation" would range from 1,000 to 50,000 or even 100,000 US dollars, depending on the scope.

## 3.2019 Parliamentary elections








### 3.1. Digital campaigning methods and practices: an overview

When a sudden dissolution of the Parliament on May 21, 2019, by newly elected President Zeenskyy gave the parties little break between the two election cycles, they quickly reoriented towards Parliamentary elections, often reusing the same people, online platforms, and campaigning methods. In particular, the parties again turned to Facebook, now the most popular social network in the country with about [14 million users](#). At the same time, parties and candidates also actively used Instagram ([11 million users in 2019](#)), YouTube, Twitter, messaging platforms such as Viber and Telegram, and even custom-made mobile applications.

In terms of digital campaigning methods, parties actively used online advertising capabilities of various online platforms, from Facebook and Instagram to YouTube and Google. According to a digital political marketing consultant interviewed for this report, parties took full advantage of such targeting instruments as Facebook's [Lookalike Audiences](#) and [Custom Audiences](#), measuring impact via backend advertiser data and promoting especially well-performing content further. Given the small audiences the parties targeted, there has been little use of such instruments as A/B testing, be it for online ads or e-mail marketing; besides, not every party

even used an automated CRM system given how expensive those can be and how much effort it would require to adapt them to a Ukrainian market.

**Summary table of our findings regarding five parties’ use of digital platforms\* for election campaigning**

| Party                          | Web-site |  |  |  |  |  |  | Other  |
|--------------------------------|----------|---|---|---|--|---|---|--|
| Sluga Narodu                   | ✓        | ✓   | ✓   | ✓   |  | ✓   | ✓   | Mobile apps  |
| European Solidarity            | ✓        | ✓   | ✓   | ✓   | ✓  |   | ✓   |  |
| Batkivsh-Chyna                 | ✓        | ✓   | ✓   | ✓   |  | ✓   | ✓   |  |
| Holos                          | ✓        | ✓   | ✓   | ✓   | ✓  | ✓   | ✓   |  |
| Opposition Platform — For Life | ✓        | ✓   | ✓   |   |  |   |   |  |

\*Images: Creative Commons

**Servant of the People** (Слуга народу)<sup>1</sup> has maintained the [most subscribers on social media](#) (including over 256,000 on Facebook by the 2019 election day<sup>2</sup>) and was third in terms of engagement at the beginning of 2020. Servant has even referred to itself as “[an Internet party](#),” indicating that it actively operates online. During the elections, its social media marketers have been credited with [bringing politics to Instagram and Telegram](#) from the platforms Ukrainians are more accustomed to, like Facebook and Twitter. Servant was particularly active on Facebook during the election campaign, focusing on user engagement — a continuing trend from the Presidential campaign — and was third in terms of spending on political ads on Facebook among the five Parliamentary parties. It also actively used the main page to promote its accounts on other platforms. For instance, the party would frequently ask users to join its

<sup>1</sup> Servant of the People is a [centrist](#) political party named after the eponymous comic TV series starring Volodymyr Zelenskyy, current President of Ukraine.

<sup>2</sup> According to Facebook monitoring by OPORA.

main Telegram channel to receive the latest updates or to use its Telegram bots to receive basic information about the party (Image 1), to submit fakes, or to report election irregularities.



Image 1: June 20, 2019, Servant of the People Facebook post announcing the creation of Telegram “help” chatbot, screenshot 14.03.2020

The party encouraged supporters to create regional Facebook pages or Telegram channels that would later be promoted through the main page to get even more users to join (many of those had been active since the Presidential campaign) and created webpages for its candidates in single-mandate districts. It also operated a separate website for debunking fakes reported by supporters — an initiative that was also launched during the Presidential campaign and proven to be extremely popular with social media users. Another novelty of this campaign by Servant was the launch of a [mobile application](#)<sup>3</sup> (available for [iOS](#) and [Android](#)) to engage with voters.

**European Solidarity** (Європейська солідарність)<sup>4</sup> had [over 400,000](#) subscribers on social media as of the beginning of 2020 (including 303,000 on Facebook by the 2019 election day<sup>5</sup>) and has been among the leaders in engagement. It also followed Servant of the People’s suit and ran campaigns on other platforms, such as the messengers Telegram and Viber, Twitter,

<sup>3</sup> Website no longer active.

<sup>4</sup> European Solidarity is a [liberal-conservative](#) pro-European party in Ukraine.

<sup>5</sup> According to Facebook monitoring by OPORA.

Instagram, and YouTube. Having other prominent public figures in its ranks, the party actively used its main Facebook page to engage with their pages as well as to promote its accounts on other platforms (Image 2). Solidarity came second in terms of spending on Facebook political ads among the five Parliamentary parties.

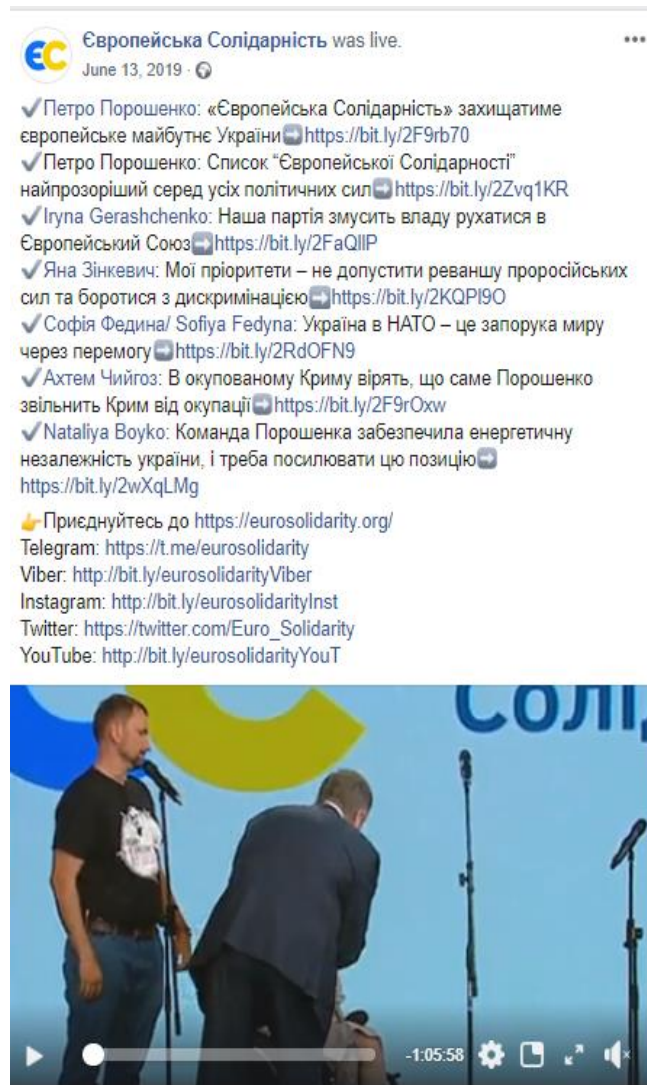


Image 2: June 13, 2019, European Solidarity's Facebook live post linking to other candidates' pages and party's social media accounts, screenshot 17.03.2020

**Batkivshchyna** (Батьківщина)<sup>6</sup>— with [over 400,000](#) social media subscribers in early 2020 (including over 341,000 on Facebook by 2019 election day<sup>7</sup>), this party ran an active campaign online, coming in fourth in terms of Facebook advertising expenses. The party also urged its

<sup>6</sup> The All-Ukrainian Union "Fatherland" or *Batkivshchyna* in Ukrainian is a [centrist pro-European](#) political party led by Yulia Tymoshenko and affiliated with the European People's Party.

<sup>7</sup> According to Facebook monitoring by OPORA.

Facebook followers to subscribe to its accounts on other social media platforms, in particular, on YouTube, as well as interacted with the page of party leader, Yulia Tymoshenko.

**Opposition Platform — For Life** (Опозиційна платформа - За життя)<sup>8</sup> has traditionally been the least active on social media, running a Facebook account with a bit over 44,000 followers by 2019 election day,<sup>9</sup> maintaining a modest Instagram account, and spending the smallest amount on digital advertising on Facebook among the Parliamentary parties. This may be explained by the party's base, which consists of older voters traditionally less active online. As for engaging with users, Platform appears to have utilized its Facebook page primarily to lead readers to the party's website (Image 3).



Image 3: June 6, 2019, Opposition Platform — For Life's Facebook post sharing a publication from party's website, screenshot 18.03.2020

**Holos** (Голос)<sup>10</sup>— a younger party on the Ukrainian political scene [with a little over 90,000 social media followers](#) (as of January 2020) has had, nevertheless, one of the highest rates of

<sup>8</sup> Opposition Platform—For Life is a [centrist/center-left Eurosceptic](#) party in Ukraine.

<sup>9</sup> According to Facebook monitoring by OPORA.

<sup>10</sup> Holos is a liberal pro-European party in Ukraine, which was led by the famous musician Svyatoslav Vakarchuk until March 2020.

engagement and utilized more social media platforms than others, including even Soundcloud. The party has paid significant attention to online campaigning, spending the most of the five parties on Facebook advertising and using the platform to urge its supporters to subscribe to the other accounts of the party on social media. It was also among the first [to create and use a Telegram bot](#) to engage with supporters. The party also used its main Facebook page to debunk “fakes” (social media posts with false information about Holos, Image 4).



Image 4: June 22, 2019, Holos's Facebook post warning followers about a social media fake (false information disseminated about the party online), screenshot 11.03.2020

### 3.2. Facebook political advertising during Parliamentary elections

Despite the fact that, according to a campaign finance watchdog’s [report](#), all Parliamentary parties had a similar spending structure during the campaign (the biggest chunk of resources was allocated to TV advertising and the second biggest to external advertising), some political forces did not report their spending on online advertisements, taking advantage of the existing legal loopholes.

Thus, in the absence of clear legal mechanisms for candidates to report or for regulators to monitor expenses allocated to Internet advertisements, Facebook’s political and social ads library recently made available in Ukraine became the only source to provide some oversight over contestants’ online spending. No other platform offered the same level of transparency.

Using Facebook’s data, domestic election watchdog OPORA established that parties ran [40,427 targeted political ads](#) during the active campaign period, spending over 1,800,000 US dollars (Image 5). At the same time, a review of parties’ interim campaign finance reports uncovered substantial underreporting of the online advertisement spending declared by the election contestants when compared against the amounts published by Facebook.

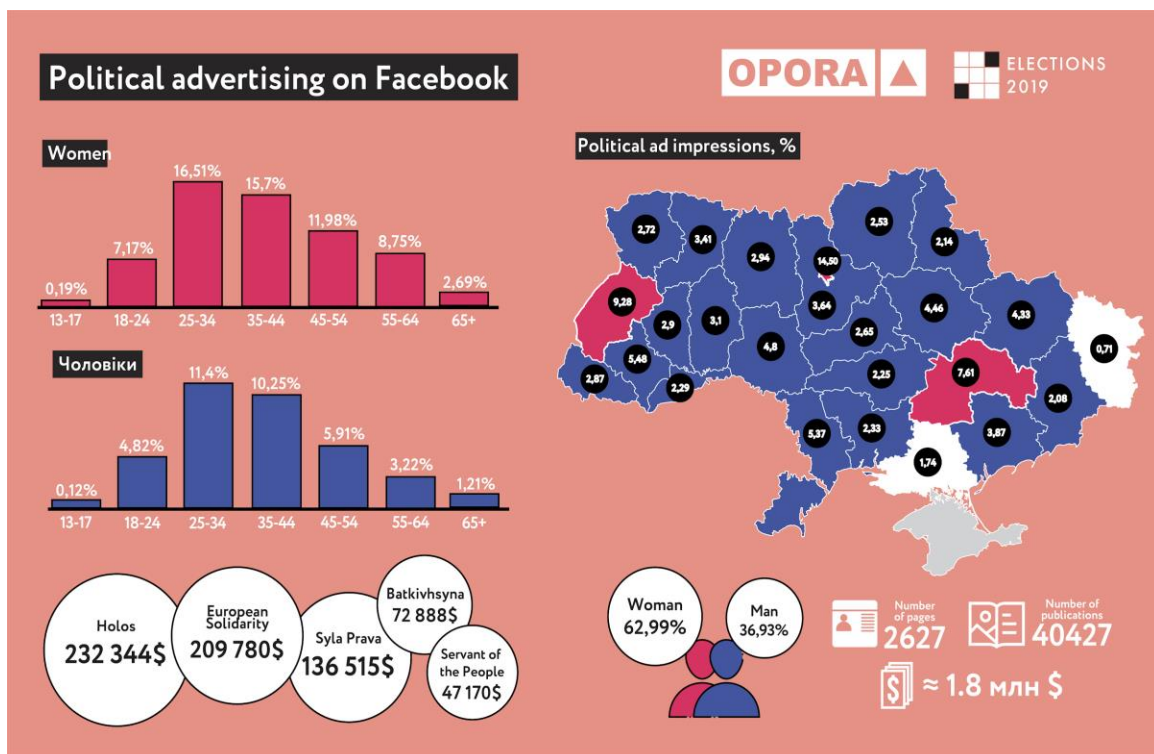


Image 5: Political ads on Facebook during the 2019 Parliamentary elections with the top five parties by spending amount, infographic by OPORA.

Although 2019 Ukrainian election legislation did not regulate campaigning on the Internet, it prohibited the use of candidates' own funds or funds from other sources for campaigning,

including voter initiatives. Therefore, third parties were not allowed to pay for advertising on social networks. However, in the absence of explicit legal prohibitions, it would be impossible to prosecute a person for campaigning on the Internet and social networks with funds outside those declared in the election fund. As mentioned above, the only way to estimate amounts parties had spent on digital advertising and from what sources was Facebook's political ads library.

According to a representative of Chesno, a movement for transparency and accountability in politics, [only three parties](#) of those participating in the 2019 elections declared spending compatible with the amounts indicated in Facebook's library of political advertisements.

Some parties, such as the Opposition Platform — For Life party, ran all its ads from the unofficial affiliate page Boyko — Prime Minister (named after one of the party leaders, Yurii Boyko). Advertising in support of the Batkivshchyna party was run from a Yulia Tymoshenko's fan page as well as her official page.

### 3.3. Other issues with digital campaigning

Similarly to the Presidential elections, OPORA recorded instances of [negative campaigning posts](#) (so-called “black PR”) published by pages not clearly affiliated with any political force. In addition, a coalition of media monitors reported that over half of political parties, including their leaders, [used hate speech elements](#) in Facebook posts aimed at discrediting their opponents during the 2019 elections.

Finally, Slidstvo.Info's investigative journalists uncovered an underground “bot farm” that offered their professional services, which included creating hundreds of fake accounts on Facebook and leaving tens of thousands of “comments” in support of or against a particular candidate. An undercover journalist [worked at the “farm” for several weeks](#), in a group that left about 40,000 comments, which may have cost election contestants as much as 20,000 EUR. While using bots is not prohibited (or otherwise regulated) by Ukrainian election law, paying for such services off the books is.

## 4. Online campaigning and data collection by five Parliamentary parties

### 4.1. Legal framework

The five parties that took seats in the Parliament in 2019, Servant of the People, Opposition Platform — For Life, the Batkivshchyna union, Holos, and European Solidarity used a variety of online methods to engage voters.

For instance, they urged voters to subscribe to mailing lists, follow their social media accounts or join groups, join messenger channels, engage with messenger bots, or install mobile applications. Most of these mechanisms would provide subscribers with information about the party and its candidates, their election platform, and the latest news, as well as basic information about voting. In addition, some parties used their websites and social media to actively recruit members, volunteers, and candidates.

Despite the growth in the use of online tools for campaigning, neither the electoral legislation in place during the 2019 elections nor the newly adopted Election Code contain regulations aimed at safeguarding the use of voters' personal data.

However, the Law of Ukraine "On the Protection of Personal Data" passed in 2010 sets mandatory requirements for all automated processing of personal data. These requirements should also apply to online voter data collection and processing practices used by political parties and candidates.

Notably, this law established enhanced safeguards for the protection of personal data related to political beliefs and membership of political parties (Article 7).

Thus, [legal regulations](#) stipulate that entities must notify the Parliament Commissioner for Human Rights (Ombudsman) about the processing of personal data, which poses a special risk to the rights and freedoms of personal data subjects (so-called sensitive data), in particular, data containing information about persons' political, religious or ideological beliefs and membership in political parties and/or organizations, trade unions, religious organizations, or public organizations of an ideological orientation. Nevertheless, political parties and some types of civil society organizations [are exempt from this requirement](#) when the data concerns their members that willingly provided personal data to the organization. It is unclear, however, what should be done about the data of non-members, such as volunteers, supporters, and other voters, collected by the political parties during an election.

In the course of writing this report, we submitted a formal request for information to the Office of the Ombudsman in Ukraine and received a response that none of the five Parliamentary parties provided such notification in 2019. Additionally, we have not found any public records indicating that such notifications were submitted by any of the five parties since the norm first came into effect in 2014.

Nevertheless, based on these safeguards and other regulations, voters' personal data should only be processed by political parties after the data subject provides unambiguous consent to the processing of their data and parties ensure its adequate protection and that the personal data is not transferred to a third party without the consent of the voter.

Article 6 of the Law on Protection of Personal Data also establishes that the processing of personal data must be carried out for specific and legitimate purposes and with the consent of the data subject. The data subject should also be able to withdraw their consent to data processing or be able to consent to any changes to its original purpose.

Consent — the primary basis for electronic processing of personal voter data for political campaigns under the Personal Data Protection Law — must comply with the following principles and must be:

- *Voluntary* — the voter should be able to decide at their own discretion what information they provide;
- *Unambiguous* — implies the need to personally put the mark in the respective checkbox or manually enter personal data on the site;
- *Informed* — the user must receive comprehensive information about what personal data will be processed, by whom, the purpose of processing, what methods and means will be applied, how this data will be used, whether it will be shared with others, and if it is, with whom and for what purpose.
- *Preliminary* — processing of personal data should not be carried out until the instance of obtaining consent (for example, until the user ticks off the respective box on the website).

Article 12 states that the user must obtain information about the entity that collects their data, the composition and content of collected data, the purpose of the collection, and the persons to whom the personal data is transferred at the time of such data collection.

Article 24 provides for the obligation of those who process personal data to protect that data from accidental loss or destruction or from unlawful processing, including unlawful destruction or access to personal data. This indicates that parties must provide technical means for protecting their own sites in order to ensure the security and integrity of user data.

## 4.2. Websites

All five parties actively used their websites for recruitment of members, candidates, or volunteers by asking users to register online by providing their full name, contact information, place of residence, and more. Based on the online calculators of the Servant of the People and European Solidarity, at least **102,000** people registered with these two parties alone.

*Our analysis of the websites and social media accounts of five Parliamentary political parties indicates that none followed all of the requirements set in the Law on the Protection of Personal Data or fulfilled all of the principles of consent when engaging voters online.*

Only two parties (Holos and Servant of the People) offered users privacy policies outlining such details as what data was being collected about them and for what purpose, whether it could be shared with third parties, how it would be protected, or what users' data rights were. Only three

of five parties asked for users' explicit consent to process their personal data collected via online registration forms (Holos, European Solidarity, and Servant of the People).

Two parties (European Solidarity and Batkivshchyna) invited users to join their mailing lists, with European Solidarity indicating that the data may also be used for "other" purposes but not providing much detail about what those might be. (It did, however, ask users to consent to the "other" use as well). Batkivshchyna used the MailChimp service to manage its mailing list but nowhere indicated that the emails would be transferred to a third-party service or asked for users' consent. The Opposition Platform — For Life party, in turn, did not specify how the data provided by users under the generic "Join" section of the website would be utilized at all.

Four of the five parties (the exception being European Solidarity) also used various analytical services that could track a person's activity across the web and share collected data with third parties, for instance, Google Analytics or HotJar. All five used cookies and trackers installed by social media platforms for advertising purposes, including Facebook, Twitter, and YouTube. Only the two parties whose websites had privacy policies attempted to inform users of such details. However, neither asked for users' explicit consent to the use of cookies (even beyond those strictly necessary for the operations of the websites) or allowed them to opt out of their information being used for marketing and advertising purposes by other platforms. None of the websites notified users about the fact that they were providing their personal data for processing from the moment they first visited the websites.

A simple inspection of the websites revealed some security issues that may indicate the breach of Art. 24, which ensures the security of user data. For instance, European Solidarity's website established an unencrypted connection with a third-party service hosting its photo gallery, while the website of Opposition Platform — For Life used a simple HTTP protocol, meaning all data provided by website users was left accessible to anyone who might monitor the connection in a plain text format.

Summary table of our findings regarding five parties' websites<sup>11</sup>

| Party  | Servant of the People (Слуга народу)                              | European Solidarity (Європейська солідарність)                        | Batkivshchyna union (Батьківщина)                   | Opp Platform — For Life (Опозиційна платформа - За життя)     | Holos (Голос)   |
|--|---|---|---|---|---|
| URL  | <a href="https://sluga-narodu.com/">https://sluga-narodu.com/</a> | <a href="https://eurosolidarity.org/">https://eurosolidarity.org/</a> | <a href="https://ba.org.ua/">https://ba.org.ua/</a> | <a href="http://zagittya.com.ua/">http://zagittya.com.ua/</a> | <a href="https://goloszmin.org/">https://goloszmin.org/</a> |
| Invites users to provide personal data (name, address, telephone and such) | ✓   | ✓   | ✓   | ✓   | ✓   |
| Has privacy policy   | ✓   |   |   |   | ✓   |
| Asks users to consent to data collection and/or processing                 | ✓   | ✓   |   |   | ✓   |
| Uses Google Analytics  | ✓   |   | ✓   | ✓   | ✓   |
| Uses Facebook's or other social media trackers                             | ✓   | ✓   | ✓   | ✓   | ✓   |
| Uses other cookies   | ✓   | ✓   | ✓   | ✓   | ✓   |
| Potential security issues <sup>12</sup>                                    |   | ✓   | ✓   | ✓   | ✓   |

<sup>11</sup> Tracker and cookie detection performed with the use of [Ghostery](#), [Cookiebot](#), Chrome cookie view function, and manual website code review.

<sup>12</sup> Only a limited analysis of websites' security was performed since complete analysis would require backdoor access to parties' websites.

A more detailed overview of each website is provided below.

The **Servant of the People** (Слуга народу) party was one of two Parliamentary parties, alongside Holos (Голос), that provided its supporters with detailed privacy policies on the party’s website and the only one of five which requested users to both accept the policies and explicitly consent to processing their personal data by ticking a separate box. Both options remained available on the “Join” page of the party’s website as of February 2020 (see Image 6).

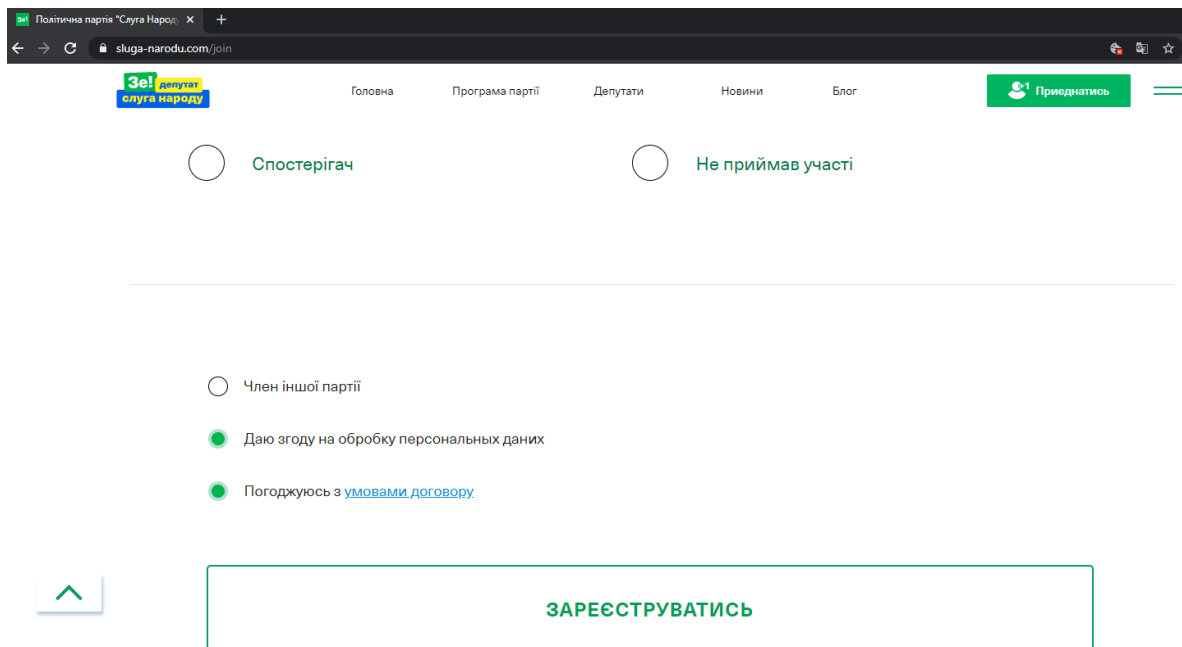


Image 6: The “Join” section of Servant of the People’s website inviting users to register with the party, screenshot 24.02.2020

The party recruited volunteers, members, and candidates online. On the “Join” page of the website, users were invited to provide rather extensive information about themselves, including their full name, telephone number, e-mail address, and the full address of a declared place of residence (Images 7-8). In some instances, additional personal information was collected, such as from volunteers registering to observe elections or serve on election commissions. As of July 16, 2019, **50,665 people** had already filled out the registration form according to the website’s online calculator.

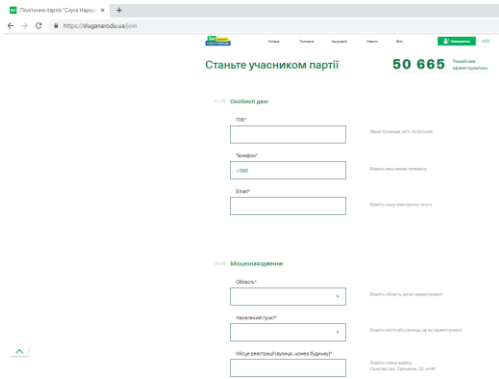


Image 7: Servant of the People’s website, “Join” section fields for entry of personal data, screenshot 16.07.2019

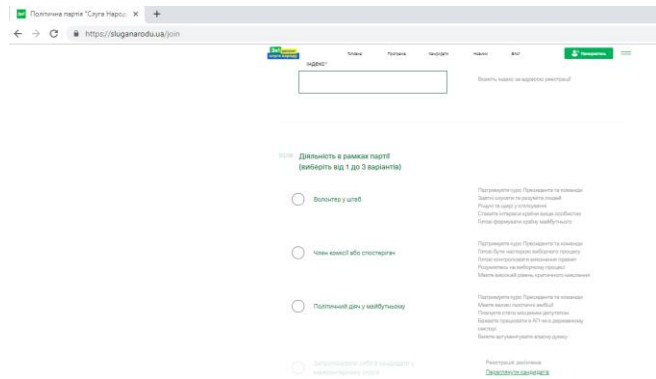


Image 8: Servant of the People’s website “Join” section fields for entry of personal data (continued), screenshot 16.07.2019

Servant’s Privacy Policy ([version as of May 25, 2019](#)) outlined the ways and types of information collection about users (i.e., information provided by users upon registration, data collected from visitors via Google Analytics, and data collected through cookies), collection purpose, and instances in which the information could be shared with third parties. It also outlined the rights of users regarding their data, for example, the right to access the data collected about them by the party. Although the Privacy Policy notes that “Data that is being collected via Cookie files cannot be disclosed to third parties. This data will not be transferred to third parties in an unauthorized manner,” the website allows for third-party cookies that track users’ activity across the web and shares the information with such platforms as Facebook. As mentioned above, users were not informed about this at the moment they visited the website, but only if/when they read the Privacy Policy.

**European Solidarity** (Європейська солідарність) appears to have had two websites during the election campaign, with only one appearing in the description of its official Facebook page and the other redirecting us to the “main” site upon attempts to access its archived version. Therefore, we only inspected what we deemed to be the “main” site, through which the party also collected voter information. Thus, on this website, Solidarity operated only one registration form, asking users to provide their full name, a telephone number, and an email address (see Image 9). Upon submission of the form, users had to tick a box confirming their understanding that the data they provided was correct and could be used “for mailing and other [purposes].” Nowhere on the website could we find a clarification for what these other purposes may have entailed or further details about the party’s use of visitors’ personal data, which violates the principles of consent outlined above. The website did not appear to use Google Analytics during the analysis, but it allowed marketing cookies from Twitter. As of the July 21, 2019, election day **52,627** users had filled out the “Join!” form, according to the party’s own tracker.

https://eurosolidarity.org

# ПРИЄДНУЙСЯ!

Ім'я та прізвище

Номер телефону

Електронна адреса

■ Я ПІДТВЕРДЖУЮ, ЩО МОЇ ДАНІ Є КОРЕКТНИМИ ТА ВОНИ МОЖУТЬ БУТИ ВИКОРИСТАНІ ДЛЯ РОЗСИЛКИ ТА ІНШОГО

НАДІСЛАТИ

*Image 9: European Solidarity's website, "Join!" registration form with consent box, screenshot 15.07.2019*

**Batkivshchyna's** (Батьківщина) website offered users an option to "Join" by becoming a party member or a volunteer and to subscribe to its mailing list. Volunteers could register online by providing their full name, a phone number, their region of residence, and whatever additional information about themselves they deemed relevant (Image 10), with the form distinguishing between mandatory and non-mandatory fields. Prospective party members could provide similar information about themselves online and were also required to deliver a filled-out paper application to the nearest party office. Before registering, they were invited to review the party's statute and its election platform.

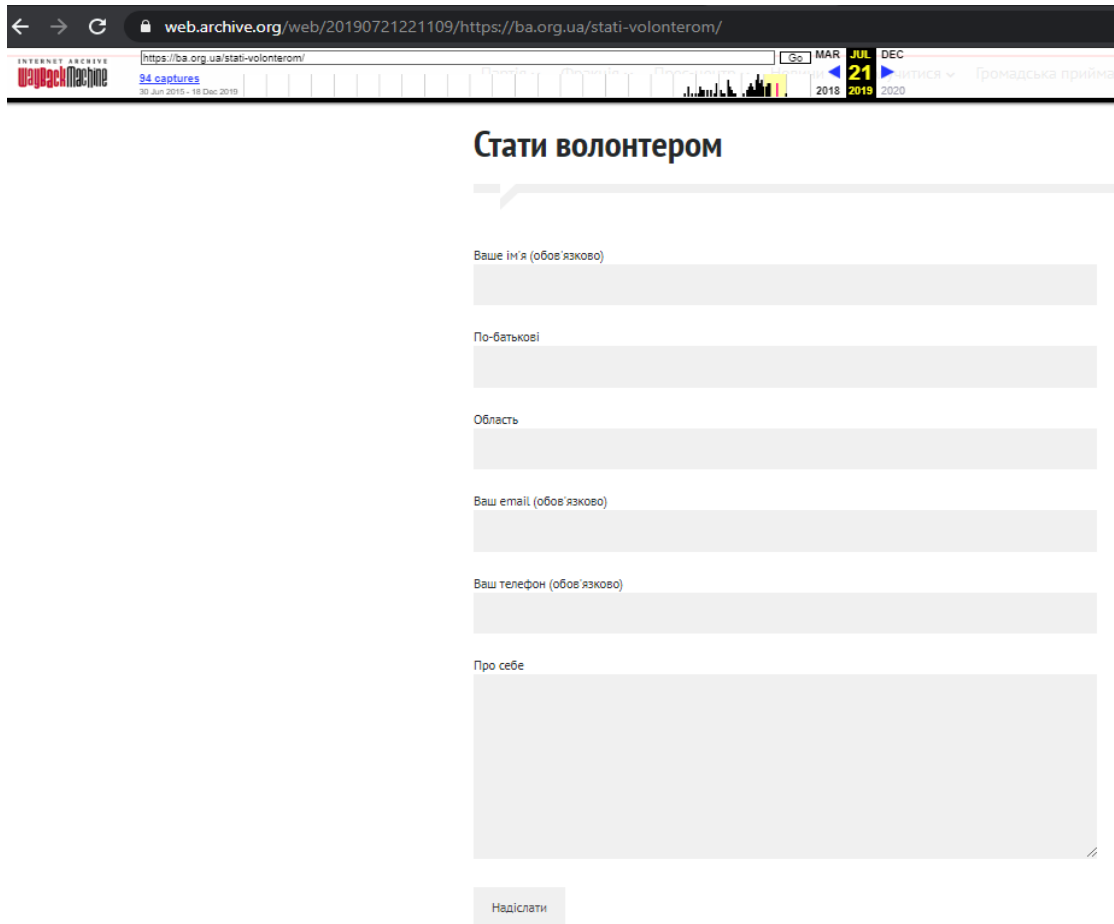


Image 10: Batkivshchyna's website, "Become a volunteer" registration page, archived 21.07.2019, screenshot 4.03.2020

Those who wished to subscribe to the mailing list had to simply enter their email address. Upon submission, they would see a standard MailChimp disclaimer confirming that their address had been registered in the electronic mailing service (Image 11). Although the act of personally filling out such a form implies a user doing so voluntarily and with an understanding of the purpose, nowhere did the party inform them how the data would be processed from users that filled out a "form," nor could we find anything resembling a privacy policy on the website. Retrospective inspection of the website's archived versions indicates that it used Google Analytics, and current analysis showed a number of cookies associated with other social media platforms (such as YouTube).

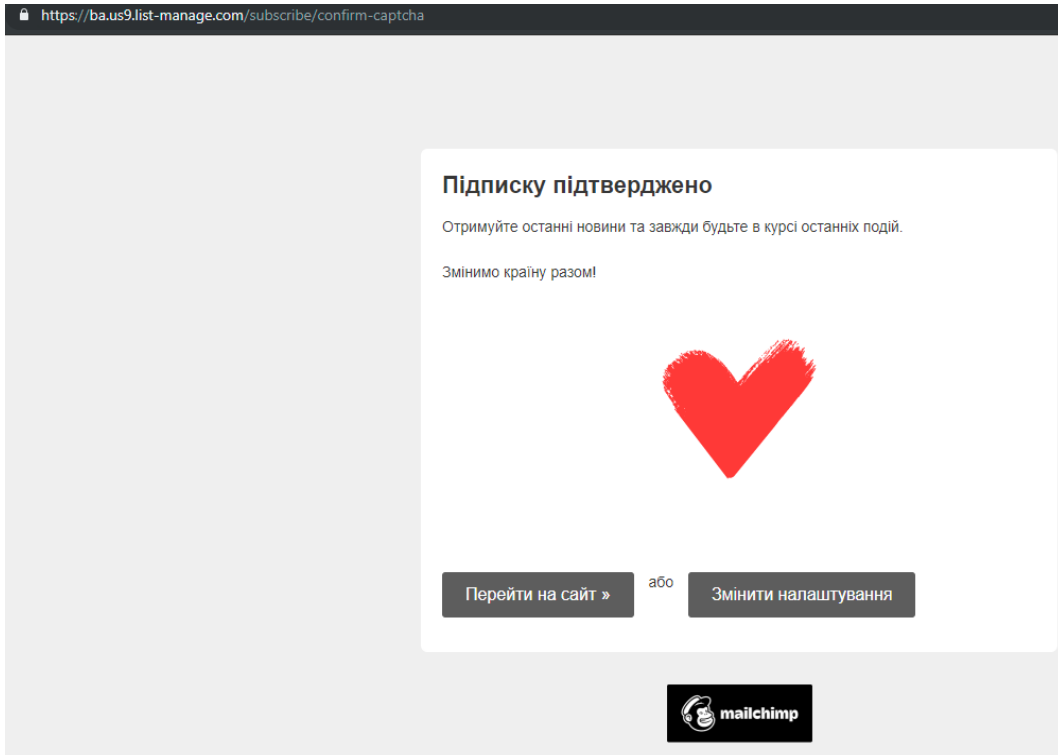


Image 11: Batkivshchyna's website, mailing list sign up confirmation from Mailchimp, screenshot 21.07.2019

**Opposition Platform — For Life** (Опозиційна платформа - За життя) operates two websites, but only one of them was (and remained) active during elections, while the second appears to be under construction and asks visitors to refer to the active one. Hence, this report analyzes only the active site.

During the campaign period, the “Join” button on the website opened a pop-up registration form asking users to provide their full name, a telephone number, their city of residence, and a few words about themselves. It was unclear in what capacity one would “join” by filling out the form (Images 12-13).

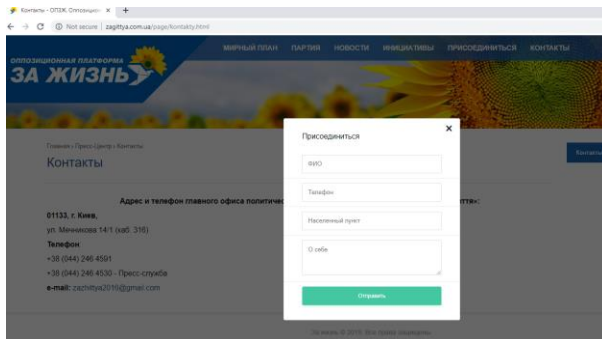


Image 12: Opposition Platform — For Life, “Join” section with a pop up registration form, screenshot 16.07.2019

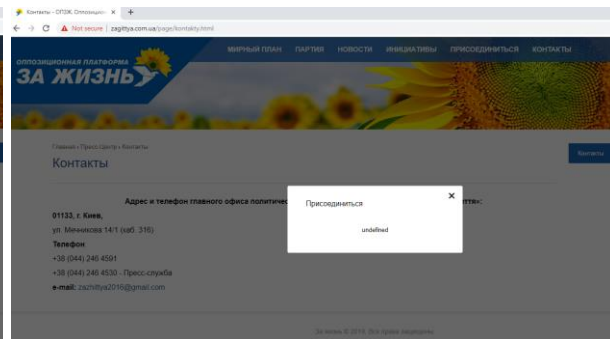


Image 13: Opposition Platform — For Life, “Join” section registration confirmation, screenshot 16.07.2019

A retrospective analysis of the website (version archived on Feb. 24, 2019) uncovered a separate option to join the party via an online registration form that asked for more detailed information (although we could not confirm that this option was enabled during the election period). In order to become a member, a user had to provide rather detailed information about themselves, including their full name, exact address of residence, occupation, date of birth, a telephone number, and an email address and would need to confirm their intention in a separate field. Most fields were marked as mandatory (Images 14-15). The party noted that the user was to familiarize themselves with its statute and platform before applying.

Отже, для того, щоб стати членом політичної партії «За життя», вам необхідно заповнити форму, надавши такі дані:

1. П.І.Б. (прізвище, ім'я, по батькові)
2. Дата народження
3. Домашня адреса (обов'язково вказати індекс)
4. Телефон (за бажанням)
5. Електронна адреса (за бажанням – якщо ви хочете отримувати розсилку новин, анонси заходів та іншу інформацію із життя Партії)
6. Соціальний статус (професія)
7. «Я хочу долучитися до лав партії «За життя»»

Якщо ви не отримали відповідь, або з якихось інших причин отримали відмову, повідомляйте про це на електронну пошту [zazhittya2016@gmail.com](mailto:zazhittya2016@gmail.com) головного офісу політичної партії «За життя».

**УВАГА! Всі поля, вказані у формі, заповнювати ОБОВ'ЯЗКОВО!**

Прізвище\*

Ім'я\*

По батькові\*

01.01.1999

Почтовий індекс\*

Область\*

Район\*

Названіе населенного пункта\*

Image 14: Opposition Platform — For Life, Member registration page with fields for entering personal data, archived 26.02.2019, screenshot 4.03.2019

web.archive.org/web/20190226185407/http://zagittya.com.ua/candidates

INTERNET ARCHIVE Wayback Machine

120 captures 19 May 2017 - 28 Aug 2019

JAN FEB 26 APR 2018 2019 2020

ІНІЦІАТИВИ ДОЛУЧ

Название населенного пункта\*

Название улицы\*

Номер дома\*

Номер квартиры\*

380

Email\*

Професія\*

Повідомлення

Долучитися до партії

Поля із \* обов'язкові для заповнення

Image 15: Opposition Platform — For Life, Member registration page with fields for entering personal data (continued), archived 26.02.2019, screenshot 4.03.2019

Retrospective analysis also indicated that the website had been using Google Analytics and a tracker from the Ukrainian entertainment portal and email service provider Bigmir.net. Nowhere on the website could we find a privacy policy or a consent box regarding processing visitors' personal data.

The **Holos** (Голос) party offered the most detailed [Privacy Policy](#) out of the two that did from the five analyzed for this report. It is currently unavailable on the party's website. Therefore, we analyzed the version [archived](#) on Election Day, July 21, 2019. For instance, the policy covered which data was and was not being collected, for what purpose, and the duration of storage for such data. Additionally, it listed third-party analytical services and cookies in use (including those by Facebook, Twitter, and other social media platforms, Google Analytics services, and others) and even instructed users how to disable them. Finally, the party outlined the rights of users regarding their data, for example, the right to access data collected by the party about themselves. We could not retrospectively confirm which trackers were being used during the election period; currently, the website uses the analytical services of Google Analytics and Hotjar as well as cookies operated by Facebook that track the behavior of the user across the web for advertisement purposes. However, the user would only become aware of this if they were to read the privacy policy and not immediately upon visiting the website.

During the active campaign period, the party recruited members, candidates, and volunteers online (Image 16), including election observers (Image 17).

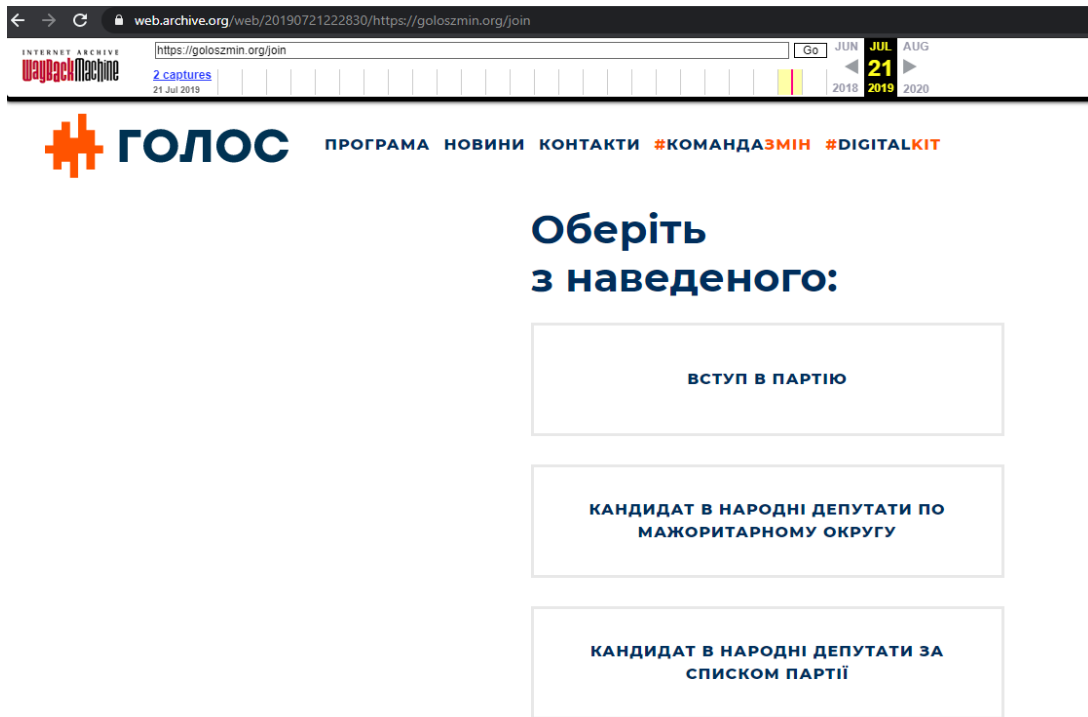


Image 16: HoloS website, "Join" section listing options of applying to become a party member, a majoritarian party candidate, or a party list candidate, archived 21.07.2019, screenshot 4.03.2020

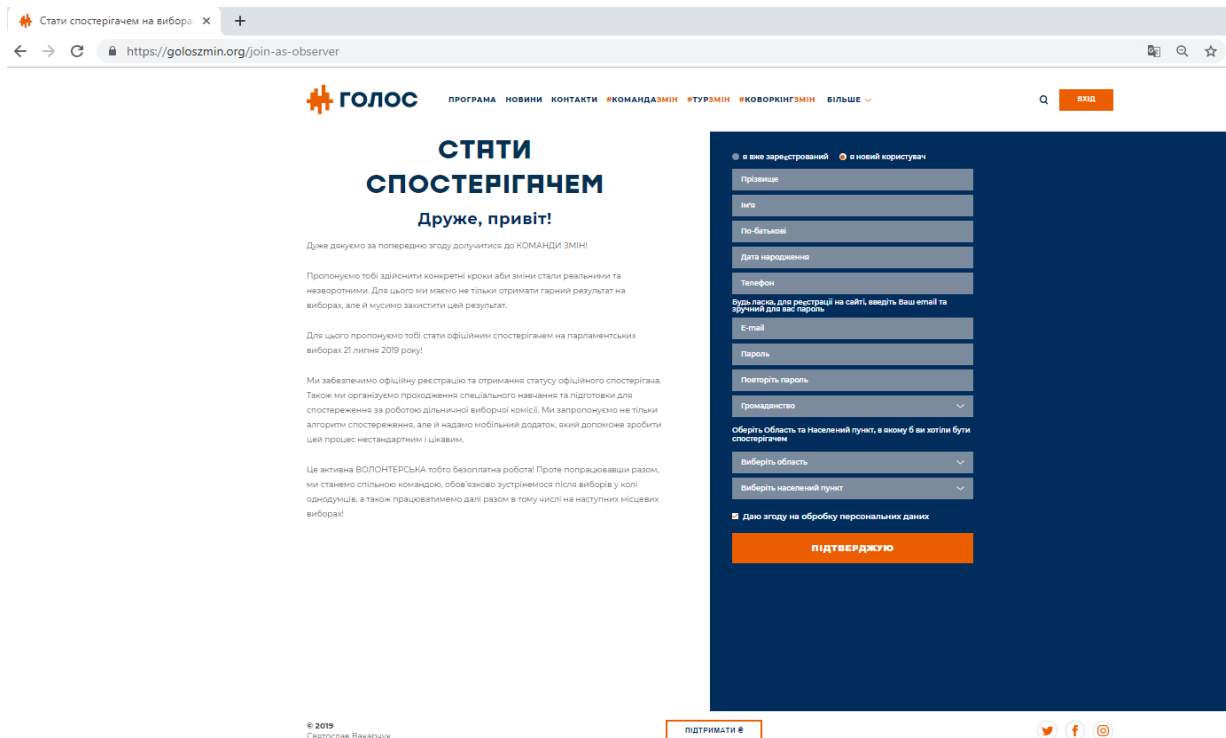


Image 17: HoloS website, registration form to become an observer, screenshot 16.07.2019

All users were first asked to complete a generic registration form by providing their region and city of residence, name, telephone number, and email address. Once registered, they could access an internal version of the website using their login credentials. The same generic registration form was still available on the website as of March 2020 (Image 18).

golozmin.org/golos

**ГОЛОС** ПРОГРАМА НОВИНИ КОНТАКТИ #КОМАНДАЗМІН ГОЛОС.КИЇВ

# ТВІЙ ГОЛОС ЗМІНЮЄ ВСЕ

Виберіть область

Виберіть населений пункт

Ім'я

Телефон

Пошта

**ПРИЄДНАТИСЬ**

Або через:

**Привіт!**  
Вітаю на сайті команди справжніх змін!  
Приєднуйся до наших активностей, приходь на івенти, запрошуй друзів!  
Ми всім щиро раді )  
**Чекаємо на тебе!!**

Image 18: Holo website, a generic registration form for “joining” a party with fields to allow the user to enter their region and city of residence, name, phone number, and email address, screenshot 4.03.2020

#### 4.2.1. Website security

A limited analysis of the websites found several issues that could present a potential problem, given that all five parties used their websites to collect personal and sensitive data from their supporters. A complete analysis would require backdoor access to parties’ websites; hence, we can only speculate about the risks these issues could have posed to the websites at the time of elections.

Summary table of our findings regarding security of the five parties' websites

| Party                     | Servant of the People (Слуга народу)                              | European Solidarity (Європейська солідарність)  | Batkivshchyna union (Батьківщина)   | Opp Platform — For Life (Опозиційна платформа – За життя)  | Holos (Голос)   |
|---------------------------|---|---|---|--|---|
| URL                       | <a href="https://sluga-narodu.com/">https://sluga-narodu.com/</a> | <a href="https://eurosolidarity.org/">https://eurosolidarity.org/</a>   | <a href="https://ba.org.ua/">https://ba.org.ua/</a>   | <a href="http://zagittya.com.ua/">http://zagittya.com.ua/</a>  | <a href="https://goloszin.org/">https://goloszin.org/</a>   |
| Potential security issues | None found  | <ul style="list-style-type: none"> <li>• <a href="#">Photo gallery webpage</a> loaded and requests were made to third party hosts without encryption.</li> <li>• Used older Wordpress version 5.2.1 with known at the time XSS vulnerability, according to archived version of the website as of July 2019</li> <li>• Used older version of JQuery - JavaScript library, according to the archived version of the website as of July 2019.</li> </ul> | <ul style="list-style-type: none"> <li>• Used outdated JQuery UI version 1.1.11 with known XSS vulnerability (according to the archived version of the website as of July 2019).</li> </ul> | <ul style="list-style-type: none"> <li>• Unsecured connections (website does not use https protocol).</li> </ul> | <ul style="list-style-type: none"> <li>• Used CMS that may have been vulnerable to a number of attacks, including XSS and RCE in the past.</li> <li>• Uses a severely outdated webserver Apache 2.4.29 with one of the critical CVE.</li> </ul> |

**Opposition Platform — For Life's** website [was using a non-encrypted HTTP protocol](#), which is considered to be insecure, potentially leaving all data submitted by users online visible to unauthorized parties should they monitor the connection. The Common Vulnerabilities and Exposures (CVE) database indicates that the server software was [somewhat outdated](#) during our review in May of 2020 but did not point to any other issues during elections. However, the connection to the website remained unencrypted at the time of writing this report.

The archived version of the **European Solidarity** website [as of July 21, 2029](#), indicated usage of the older WordPress version 5.2.1, an XSS vulnerability known at the time, which could allow unauthorized third parties to trick users into providing their personal data. However, this vulnerability could be mitigated by website administrators. The same applies to an older version of JQuery, version 1.12.14 - JavaScript library.

The archived version of **Batkivshchyna's** website [as of July 21, 2019](#), showed usage of outdated JQuery UI version 1.1.11 with the known [XSS vulnerability](#). Other known vulnerabilities may have led to denial of service but not to a user data/input compromise.

The CMS used by **Holos's** website may have been vulnerable to a number of attacks, including XSS and RCE in the past. However, the exact vulnerabilities remain unknown to us. Our review in May of 2020 revealed that the party was using a severely outdated Apache 2.4.29 webserver with one of the [critical CVEs](#). Additionally, historical DNS data shows that from May 1, 2019, till November 15, 2019, the party hosted their website on a shared hosting platform provided by OVH, which made them especially exposed to the mentioned vulnerability.

The Law on Protection of Personal Data stipulates that increased safeguards should be applied to personal data indicating persons' political views or affiliations (Article 7). Additionally, Article 24 provides for the obligation of entities that process personal data to protect such data against accidental loss or destruction and from unlawful processing, including unlawful destruction or access to personal data. Thus, political parties should ensure the security of their websites that would realistically prevent voters' data from being intercepted or lost.

We may speculate that such protection would entail the use of secure protocols, updated software, and so on. However, the law does not define the exact security measures that should be put in place, nor does it clarify, akin to the GDPR<sup>13</sup>, that the measures should be ["appropriate" to the risks](#) presented by the processing of such data. In turn, the parties are left to their own devices when it comes to website security or the security of other online tools. Given that many competing priorities amidst finite resources are a defining feature of any election campaign, it is somewhat predictable that implementing security measures may not always take precedence. Additionally, there is a low awareness of digital security's importance during an election, and only a few resources are freely available to all political parties that provide [basic guidelines on digital security for campaigns](#) or offer [checklists for ensuring website security](#).

Notably, four days after the elections, the **Holos** (Голос) party [announced](#) that its CRM server experienced a cyber-attack by a loose group of hacker-activists called the Ukrainian Cyber Alliance (UCA), best known for hacking Russia-backed militants in Ukraine's Donbas region, attacking Russian online propaganda platforms, and [leaking the emails](#) of high-ranked Kremlin political operative Valdislav Surkov. It appears that an attack against Holos was an "unofficial" penetration test, carried out within the framework of the ongoing [#FuckResponsibleDisclosure campaign](#) aimed at publicly shaming Ukrainian public officials for not implementing appropriate

---

<sup>13</sup> The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area.

cyber security measures. Both were rather transparent about the whole ordeal, with Holos promptly revealing the details to the public (Image 19), noting that they were still investigating whether any personal details of users were leaked online and UCA confirming that discovered vulnerabilities were promptly patched by the party (Image 20).

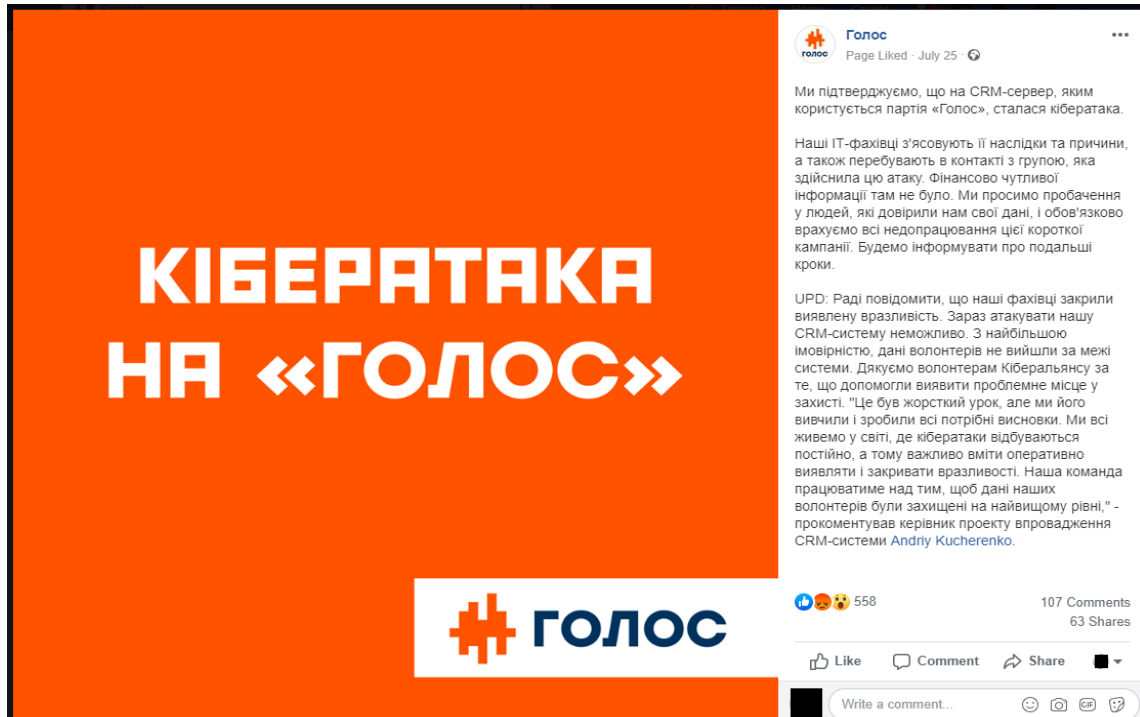


Image 19: Holos Facebook announcement about the hack, screenshot 29.07.2019

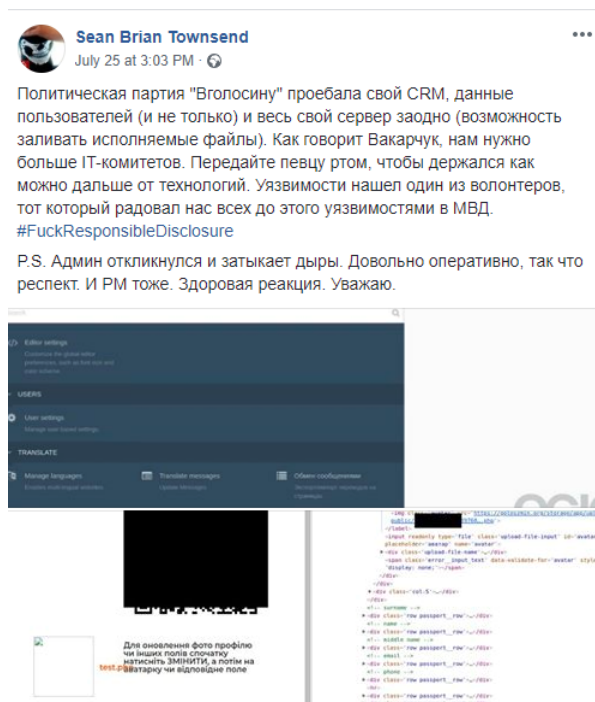


Image 20: Facebook post of a self-proclaimed UCA "Press-secretary" describing the attack, screenshot 29.07.2019

The incident makes it even more evident that, given the nature of personal data collected by the parties in 2019 and the extent of their digital campaigning, the consequences of a cyber-breach could be substantial. Those with fewer resources dedicated to security are left particularly vulnerable to attacks.

### 4.3. Other methods of data collection during digital campaigning: Facebook, Google forms, mailing lists, petitions, etc.

All five parties actively campaigned on social media, especially Facebook — on which every party ran an official page, sometimes accompanied by a cohort of semi-official or unofficial pages and groups (i.e., regional pages, pages of party leaders, fan pages, or pages of individual candidates). Parties used social media to engage voters, in particular, by asking them to provide some information about themselves that could later be used for campaigning, such as targeted online advertising or e-mail outreach.

Such means of engagement included encouraging users to subscribe to parties' mailing list, register for various events or activities by filling out a Google form, sign up for a Facebook event or create their own, sign an online petition, or follow a link to a website to apply to become a party member or a volunteer. At least two parties (Batkivshchyna and Servant of the People) activated the "Sign Up" button on their Facebook pages.

According to Facebook political ad library data [collected and analyzed by an election watchdog OPORA](#),<sup>14</sup> Holos (Голос) published the most posts calling on their supporters to register for an event on Facebook or via Google forms or a website.

*While on their websites several parties published privacy policies or requested users to consent to processing their personal data, fewer and less consistent attempts to do the same were made when collecting data via social media or other customizable tools (i.e. Google forms, online petitions, or emailing software).*

According to Facebook's own data analyzed by OPORA, **Servant of the People** (Слуга народу) spent about [47,000 US dollars](#) on targeted political advertisements on the platform, targeting more women than men with a wide geographic focus (Image 21).

---

<sup>14</sup> According to Facebook monitoring by OPORA, report publication pending.

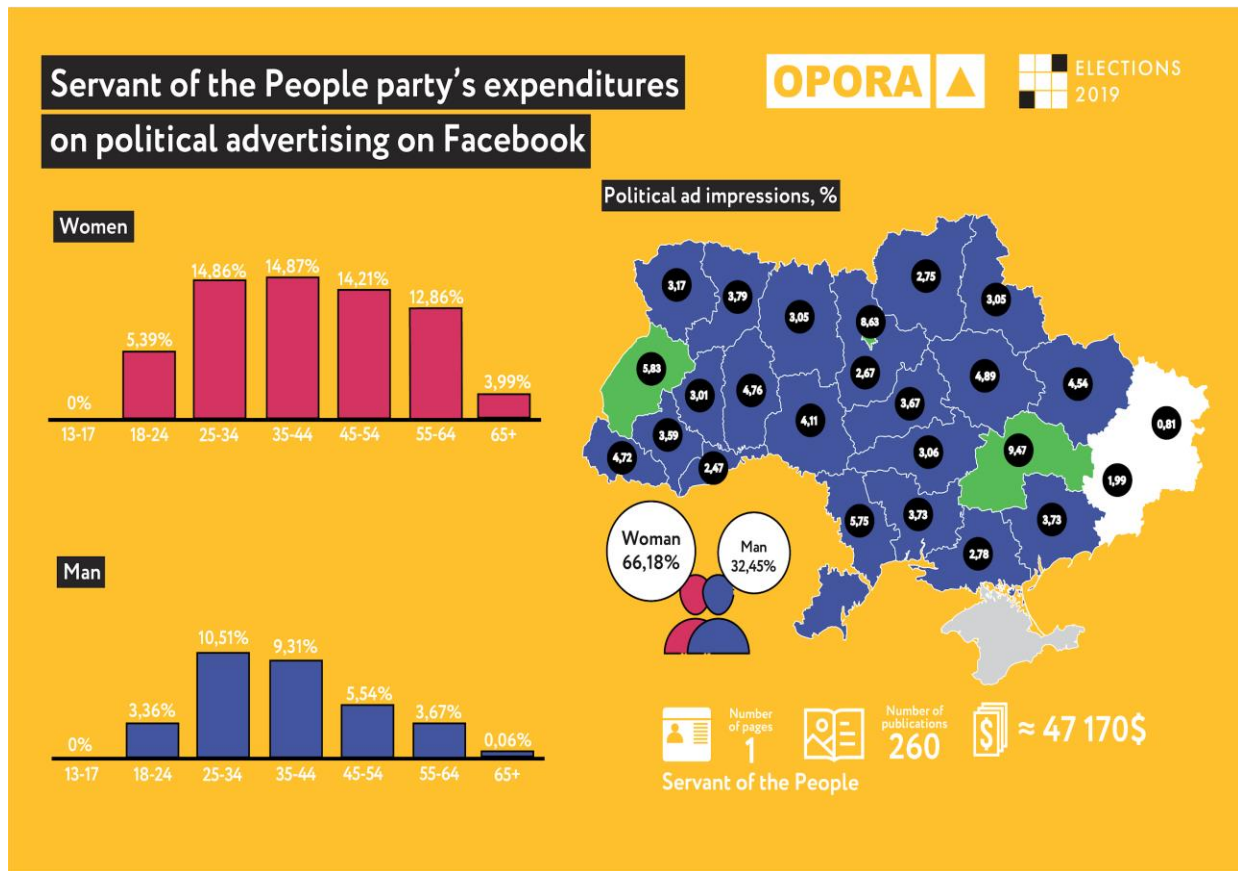


Image 21: Servant of the People political ads on Facebook during 2019 Parliamentary elections, infographic by OPORA

At the same time, of those, we found only three ads on the party's official page calling on supporters to register and report an issue of concern in their locality to a respective candidate via a mobile app or a website, costing the party between 300 and 1,500 US dollars. (More ads about the app ran on the party's regional and candidates' pages, however).

Nevertheless, the party's majoritarian candidates that also used Facebook's advertising services often encouraged their supporters to register as event attendees, volunteers, or election observers via self-created Google forms. In such cases, some candidates [included a lengthy disclaimer](#) referencing Ukraine's personal data protection norms (Images 22-24), while others simply required users to [tick a consent to data processing box](#) (Image 25), and yet others made [no such efforts](#) (Image 26).

**Зе! депутат слуга народу** **Ганна Бондар** округ 220

**Вітаю в Зе.Команді! 220 округ**

Розкажи про себе, щоб долучитися!  
Сламити не будемо  
220 округ: Виноградар, Поділ, Куренівка, Мостицький і Вітряні Гори

\* Required

**Ім'я \***  
Your answer

**Прізвище \***  
Your answer

**Твоя громада \***

- Виноградар
- Поділ
- Куренівка
- Мостицький
- Вітряні Гори

**Вік \***

- 18-25
- 26-35
- 36-45
- 46-55
- 56-65
- 66 і більше

**e-mail \***  
Your answer

**Телефон \***  
У форматі 05012345678  
Your answer

**Род зайнять \***

- студент
- працюю по найму
- підприємець
- пенсіонер
- держслужбовець
- військовий
- Other:

Images 22, 23: Servant of the People District 220 candidate's Google form used for registering campaign volunteers during 2019 Parliamentary elections, screenshot 7.05.2020.

Other:

**Оберіть як хочете допомогти! \***

- повісити банер на балконі
- розповісти про нас 10 друзям
- розкидати у своєму під'їзді нашу агітацію
- роздавати листівки біля метро та зупинок (нарайоні!)
- хочу розважатися в шатрі кандидата
- хочу прийти на пікнік
- хочу бути спостерігачем на дільниці в день голосування (всьому навчимо!)
- член ДВК (якщо ви вже маєте цей досвід)
- Other:

**\***

Я підтверджую, що відповідно до Закону України «Про захист персональних даних» добровільно надаю політичній партії «Слуга народу» свою згоду на обробку, зберігання та використання протягом необмеженого терміну моїх персональних даних згідно з цією анкетой. Своїм підписом я підтверджую, що повідомлений(а) про виключення моїх персональних даних до бази персональних даних, цілі обробки персональних даних та осіб, яким передаються мої персональні дані, а також про свої права, передбачені ст. 8 Закону України «Про захист персональних даних». Я не вимагаю здійснення повідомлення про передачу (поширення) моїх персональних даних, що включені до вказаної бази персональних даних, третім особам, якщо така передача (поширення) відбувається в моїх інтересах виключно з вказаною метою, а саме безоплатна участь в діяльності політичної партії «Слуга Народу»

Підтверджую

**Submit**

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

Image 24: Servant of the People District 220 candidate's Google form used for registering campaign volunteers during 2019 Parliamentary elections (continued), screenshot 7.05.2020.

**Волонтери команди "Слуга народу"**

Хочеш стати частиною команди "Слуга народу" в 68 виборчому окрузі (Ужгородський р-н), заповни форму і з тобою зв'яжеться наш менеджер.

\* Required

ПІБ \*

Your answer

Номер телефону \*

Your answer

Згода на обробку персональних даних \*

Підтверджую

Submit

Never submit passwords through Google Forms.

This form was created outside of your domain. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

Image 25: Servant of the People District 68 candidate's Google form used for registering campaign volunteers during 2019 Parliamentary elections, screenshot 8.05.2020

**Слуга Народу - Ігор Фріс - округ 84**

Дякуємо за небайдужість! Заповніть форму та долучайтесь до команди розвитку! Зробимо їх разом!

\* Required

Вкажіть ваше ім'я та прізвище \*

Your answer

Залиште ваш номер телефону, і ми з вами скontaktуємо \*

Your answer

Submit

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#)

Google Forms

Image 26: Servant of the People District 84 candidate's Google form used for registering campaign volunteers during 2019 Parliamentary elections, screenshot 8.05.2020.

Servant also utilized the "Sign up" button on its Facebook page to lead users to the "Join" section of the party's website described above (Image 27).

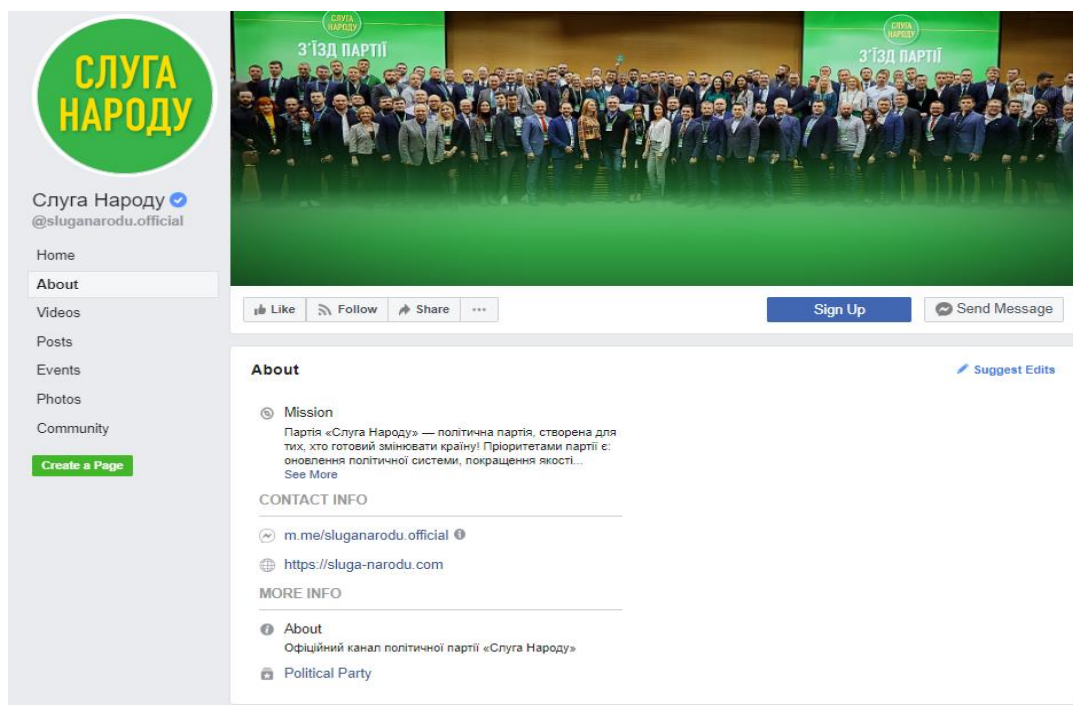


Image 27: "Sign Up" button on the Servant of the People party's official Facebook page, screenshot 19.03.2020

**European Solidarity** (Європейська солідарність) also actively campaigned on Facebook, spending over 200,000 US dollars on political ads on the platform, targeting slightly more women than men and prioritizing western and central Ukraine (Image 28).

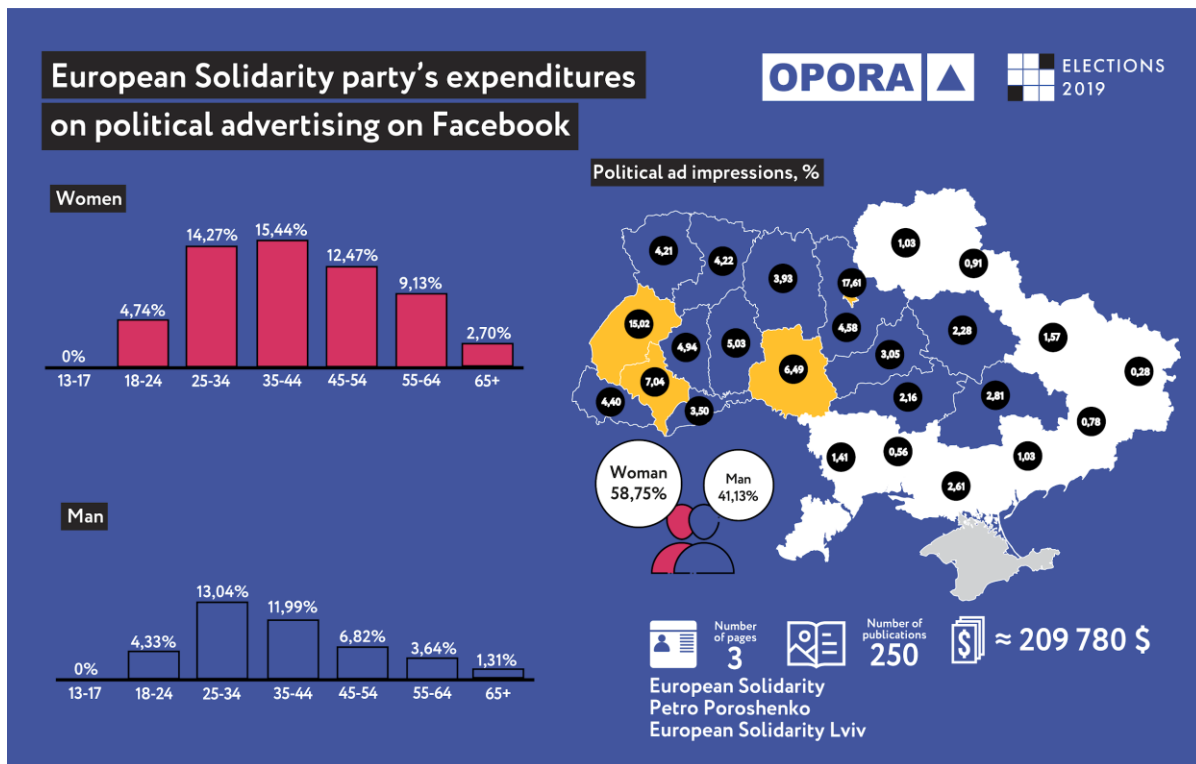


Image 28: European Solidarity's political ads on Facebook during 2019 Parliamentary elections, infographic by OPORA

Although we could not confirm whether the party used the “call-to-action” button on its page at any point of the campaign, it urged supporters to join via the website and sign up for its accounts on other social media platforms (Image 29). However, we found no promoted posts urging supporters to register with the party or otherwise leave their personal data on the party's official page and two affiliated pages that ran political ads on its behalf (Petro Poroshenko's page and European Solidarity Lviv page).

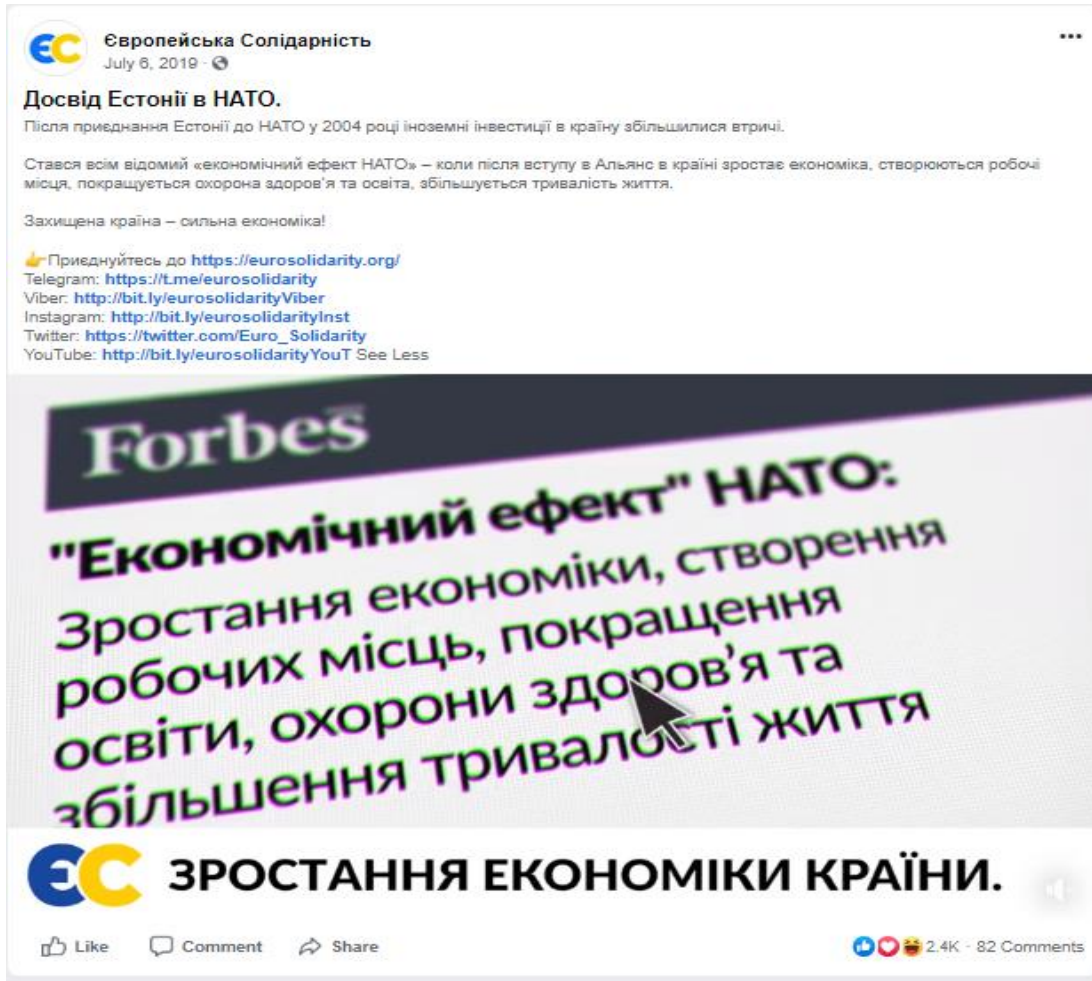


Image 29: July 6, 2019, European Solidarity's Facebook post calling supporters to join via website and other social media platforms, screenshot 16.03.2020

Nevertheless, on at least one occasion, Solidarity called on its supporters to sign an online petition urging the Parliamentary Assembly of the Council of Europe to cancel Russia's membership and voting rights. At the time of writing this report, **41,561 persons** had [signed](#) the petition started by the party, which means that it receives personal information provided by each signatory, in line with Change.org's [privacy policy](#). While Change.org believes it is necessary to share such information with petition creators to demonstrate the legitimacy of the signatures, initiating online petitions can also be utilized to collect data about the supporters of the cause and later used at their own discretion (for instance, to contact users that provided their email addresses independently of the petition platform).

**Batkivshchyna** (Батьківщина) came in fourth in terms of Facebook advertising expenses with about 72,000 US dollars (Image 30). The ads targeted more women than men, spread more or less evenly in terms of geographic focus. Looking at the party's ads (run by its leader Yulia Tymoshenko and an affiliated fan page), we found no promoted posts urging supporters to register with the party or otherwise leave their personal data.

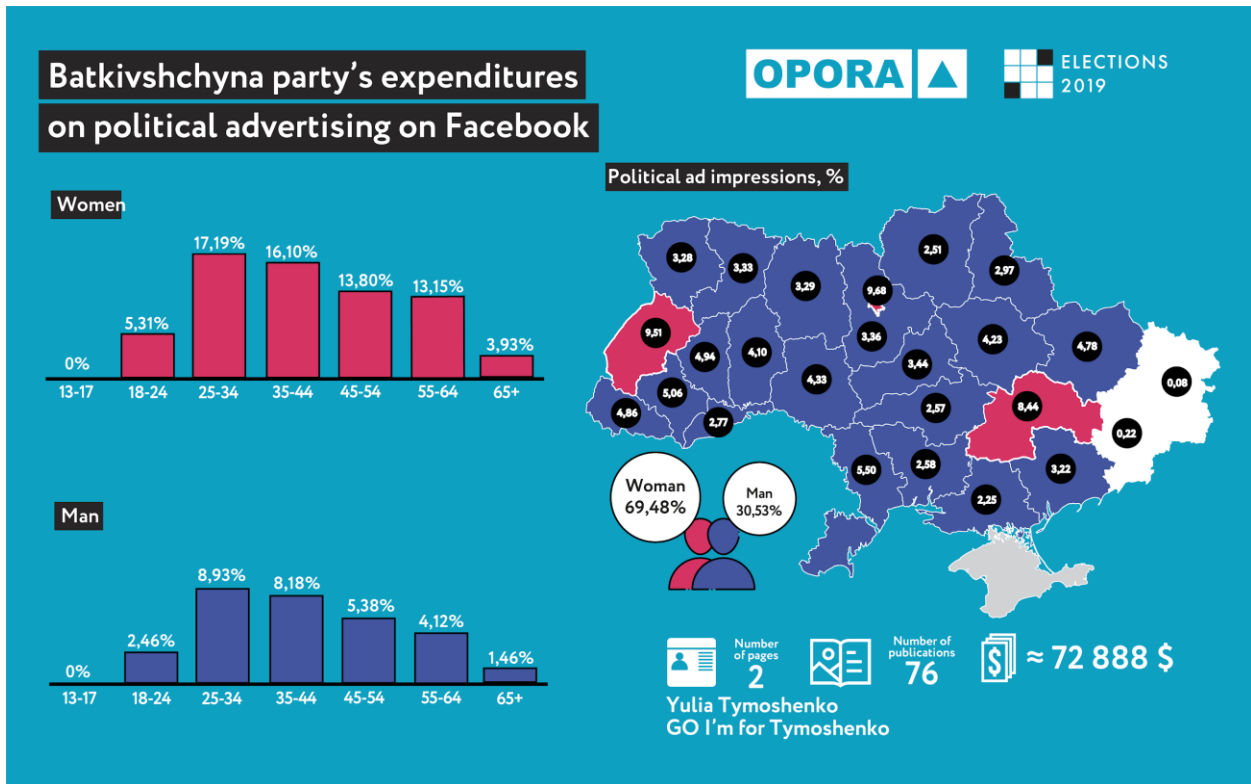


Image 30: Batkivshchyna political ads on Facebook during 2019 Parliamentary elections, infographic by OPORA

The party used Facebook's "Call-to-Action" button on its main page to prompt users to sign up to its MailChimp mailing list, the same function it enabled on its website and similarly without detailing how it would process user data. Notably, MailChimp's GDPR-compliant [privacy policies and functionality](#) include specific consent boxes pertaining to users' personal data (for example, allowing for opt-in consent from users and letting organization utilizing the software explain how they would use the data). But those functions either remained unavailable to Ukrainian users or were not enabled by Batkivshchyna (Image 31).

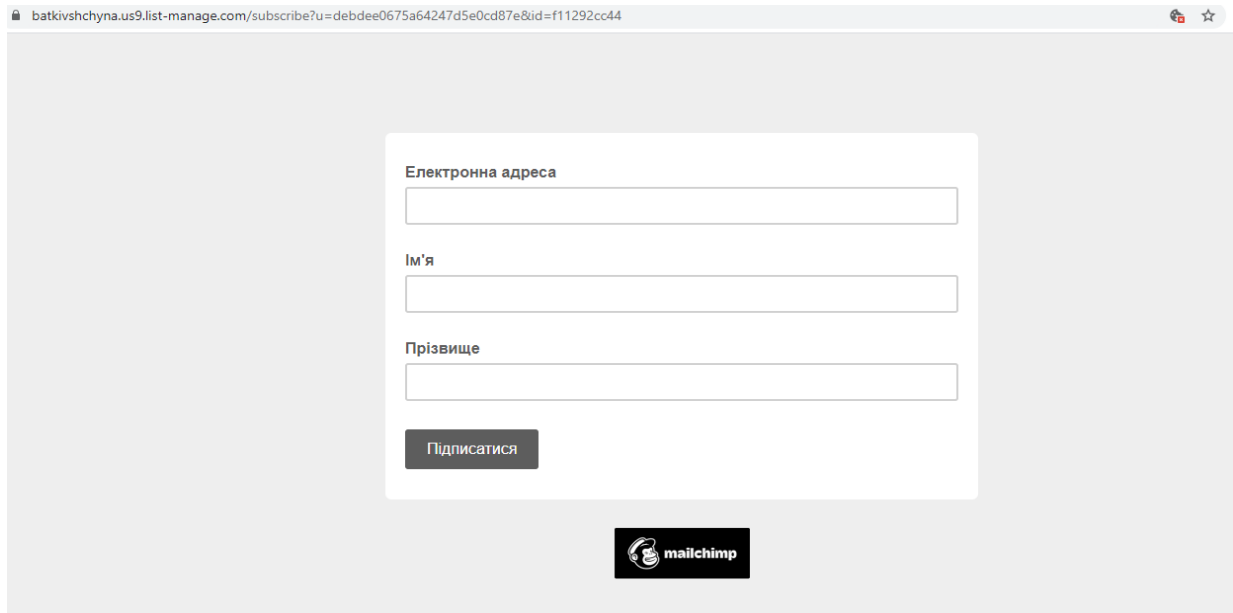


Image 31: Batkivshchyna’s Mailchimp registration form connected to Facebook’s “Call-to-Action” button, screenshot 17.03.2020

**Opposition Platform—For Life** (Опозиційна платформа - За життя) — while the least active on social media—has, nevertheless, spent over 40,000 US dollars on online political advertising, targeting Facebook users of over 35 years old (Image 32).

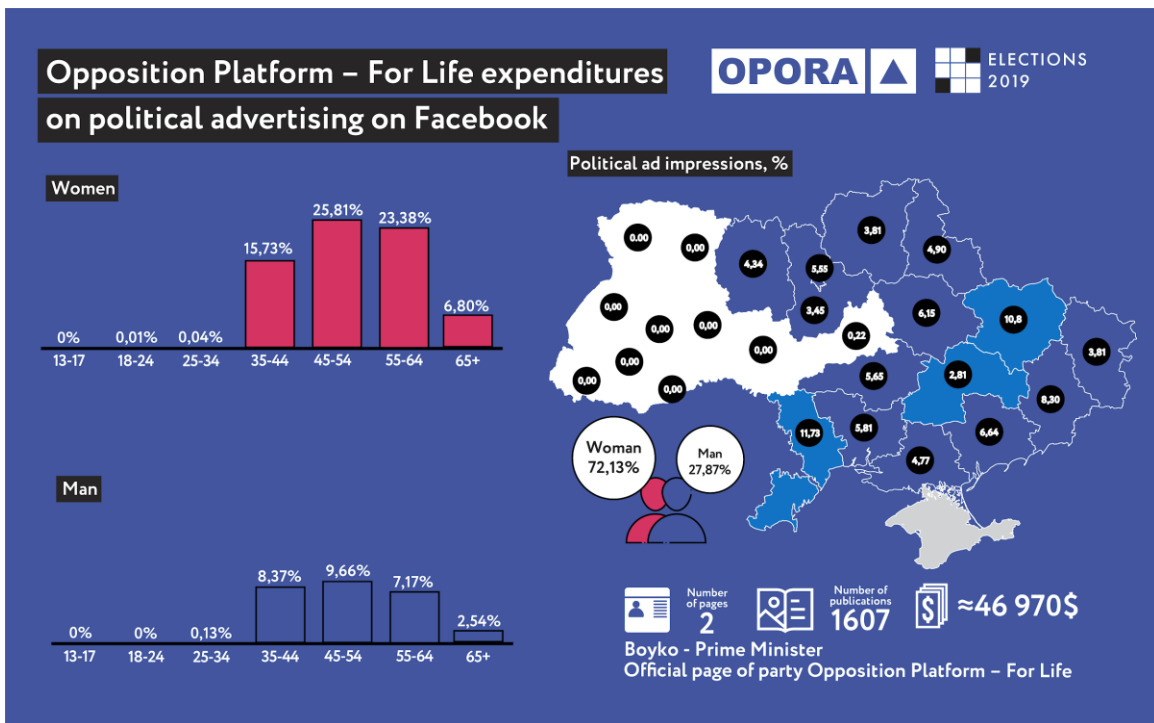


Image 32: Opposition Platform — For Life political ads on Facebook during 2019 Parliamentary elections, infographic by OPORA

At the same time, we could find no promoted posts that linked directly to its “Join” section or prompt users to register with the party in some other way, run by the party’s official page or an affiliated fan page (Boyko — Prime Minister).

**Holos** (Горос) spent the most on political advertising on Facebook, over 230,000 US dollars (Image 33), targeting the youngest audience of all parties. At least 262 promoted posts on the party's official Facebook page called on the supporters to register for something by providing their personal data, at the cost of at least 41.6 thousand US dollars.

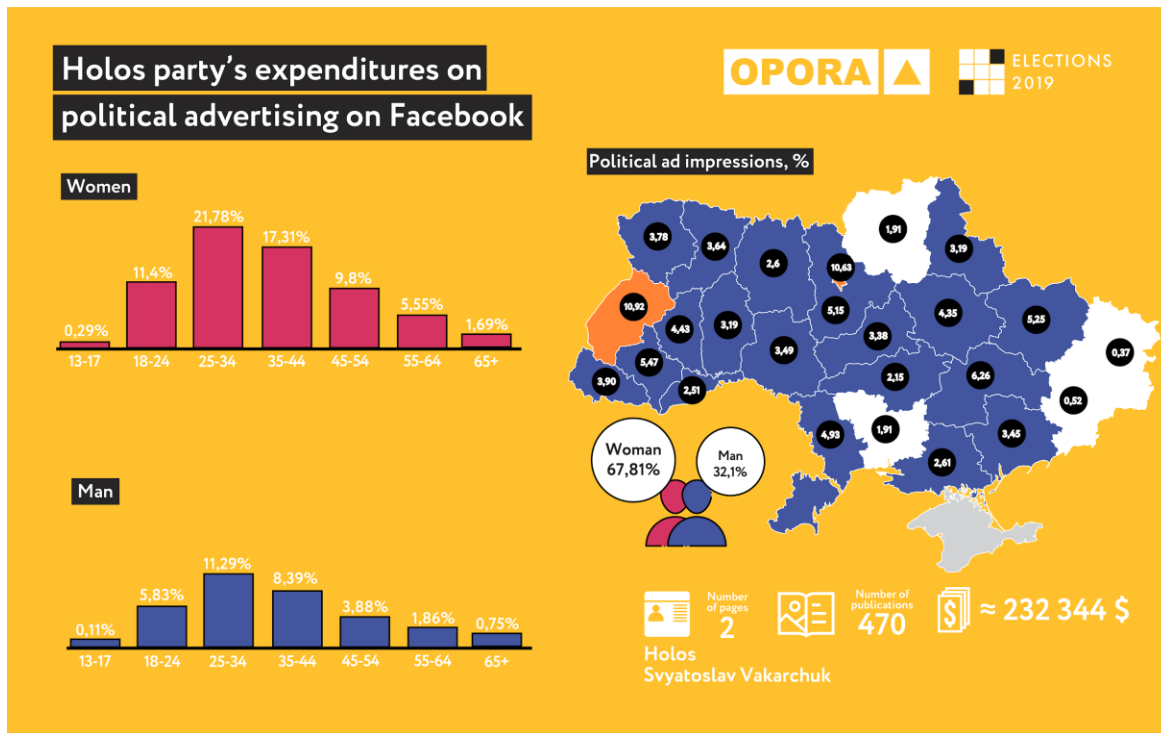


Image 33: Holos’s political ads on Facebook during 2019 Parliamentary elections, infographic by OPORA

Thus, the party frequently posted links to the registration forms on the website described above and actively focused on mobilizing supporters to [campaign on its behalf online](#). It also urged its supporters to join the party’s offline events and campaigning activities, recruiting participants via Facebook events or Google forms. The Google form-based applications for [volunteering](#), an opening of party-branded co-working space, an [application to head the co-working space](#), or the organization of a [Holos-themed party](#) that we were able to recover at the time of this research did not contain any reference to Holos’s privacy policies nor asked applicants to consent to personal data processing (Images 34-35).

Image 34 Holos party's Google form-based volunteer registration form, screenshot 22.03.2020

Image 35: Holos party's Google form-based volunteer registration form (continued), screenshot 22.03.2020

## 4.4. Messengers and chatbots

As noted earlier, the 2019 election cycle brought messenger applications such as Telegram to the forefront of parties' and candidates' online activity. Four of the five parties reviewed in this report used Telegram channels or groups for online voter outreach, and at least one used Viber. Another new feature of 2019's online engagement practices included the use of chatbots.

While Telegram channels were used for one-way communication with voters (mostly pushing updates about the parties/candidates and their activities), the messenger's API allowed third-party developers to create chat bots — automated Telegram apps for users to interact with. By engaging with such apps, users inevitably send some of their data to respective developers. The data, such as public account data and the contents of the messages, is shared with the developers during interaction with the bot. In its privacy policy, Telegram notes that other than its own bots, third-party bot developers and their apps are completely independent from the service and [should ask users for permission](#) before they access their data or users make it available to them.

Servant of the People and Holos both actively used Telegram chat bots during the 2019 campaign. For instance, Servant of the People used them to answer frequently asked questions about the party and its candidates and to crowdsource reports about election irregularities or alleged “fakes.” We interacted with two of these bots belonging to different parties, with one of them asking for the voting district of the user to provide information about the respective

candidates. Neither of the bots provided any information about data collection or asked for permission (Image 36).

Holos also used Telegram chat bots during the campaign. In particular, the party was the first to [create an open Telegram bot](#) to crowdsource reports about election irregularities from both accredited observers and regular citizens. When interacting, the party’s bot repeatedly asked a user to “register.” Further interaction, however, continued without any information about data collection or asking for user consent (Image 37).



Image 36: Servant of the People’s FAQ Telegram bot, screenshot 16.07.2020



Image 37: Holos’s election observation Telegram bot, screenshot 19.07.2020

## 5. Other sources of citizens’ personal data

A number of official and non-official databases and registries of citizen’s personal data exist in Ukraine. They include government registries compiled and administered by the state for the purposes of providing public services, consumer databases, and constructed data sets of a commercial nature whose origin is not always evident. A number of incidents when state and private databases have been found to be offered for sale online indicate that the protection of personal citizens’ data by public and commercial institutions still leaves much to be desired.

Although we found no clear evidence that political parties used such data in their 2019 campaign or tried to acquire additional data on voters from data traders, election observers recorded cases of [illegal collection and use of personal data](#) and targeting of voters according to data they [did not provide to any political force](#) during campaigning. However, at present, parties appear to be more reliant on data on their members and supporters that they have collected on their own, even if such data collection practices sometimes breach the existing legal framework

## 5.1. State Voter Registry

Perhaps a major database of voter information is Ukraine's **State Registry of Voters**. The Registry is an [automated, centralized national database](#) created by the Central Election Commission (CEC) to account for all voters nationwide in 2009, comprised of such data as the voter's full name, date and place of birth, declared place of residence, and other personal data of all persons that are of 18 years of age or older and are otherwise granted suffrage according to the law. The database is maintained by a special body within CEC with the use of appropriate security measures and allows for real-time updates as well as provides for the creation of voter lists for elections and referenda of all levels. Citizens' personal data is automatically included into the registry upon them reaching voting age, resulting in over 30 million records.

The Law of Ukraine on the State Registry of Voters provides mechanisms for public scrutiny, among them the right of a voter to review their personal information (both online and offline) and request changes if needed. The registry is also available for public scrutiny to registered [Presidential candidates](#) and [political parties](#) represented in the Parliament no later than 60 days before a scheduled election. The latest [procedure](#) prescribed by the CEC foresees providing an electronic copy of the complete registry data on a secured optical storage device to an authorized party representative or a candidate in order for them to audit created voter lists, and only for that purpose, in full compliance with the legislation on the protection of information and personal data. According to the same procedure, one designated representative per Parliamentary party or a Presidential candidate personally then may scrutinize the data on the premises of the CEC, during its working hours, using the equipment and specialized software provided by the commission, and without the right to create full or partial copies of the data in any form, including with the use of photo or video equipment.

Naturally, such strict procedure renders scrutinizing a database of over 30 million records in any meaningful way impossible. As famously claimed by one of the 2019 Presidential candidates, he would need over 6,000 years to [personally audit the registry's data](#) under the conditions stipulated above, all under the auspices that otherwise the data may be sold or leaked to an adversary. Election observers, in turn, called on the CEC to [provide depersonalized registry data in a machine-readable format](#), enabling wide public scrutiny and dispelling concerns about [possible manipulations with voter lists](#) from the side of the authorities or election contestants. Nevertheless, a court ruling has [recognized](#) such limited access to the registry to be within the norms of the law, since it is predicated on security considerations.

The security of the registry’s website was also probed by one of Ukraine’s Cyber Alliance hackers in 2018, when he [found it to be vulnerable to a cross-site scripting \(XSS\) attack](#). While the vulnerability did not appear to be critical, CEC members themselves admitted to the lack of qualified IT/cyber security personnel among civil servants due to a large pay gap between the public and commercial sectors.

## 5.2. Leaks, hacks, and security concerns

Concerns about the security and integrity of personal citizen data collected and processed by public and commercial institutions have been raised in other contexts as well. In a 2019 interview, then future Minister of Digital Transformation of Ukraine Mykhailo Fedorov [alluded](#) to certain state registries being controlled by criminal authorities—an “obstacle” in the way of the new government’s ambitious plan to digitize public services. Law enforcement authorities have also investigated cases of confidential state datasets being traded on “dark” websites, such as the database of [Ukraine’s Customs Service](#). Meanwhile, journalists have uncovered online bulletin boards with dozens of datasets containing consumer data available for purchase, such as the database of [18 million clients](#) of Ukraine’s largest logistics company or clients of one of the largest Ukrainian banks, with some data traders [offering to compile custom databases](#) containing full names, telephone numbers, gender, and email addresses upon request. Although we have no possibility to verify the authenticity of some of the datasets still available online, the file names suggest that they may have originated from state bodies or major commercial entities of Ukraine. One recent media investigation into the issue concluded that [data from a unified state demographic registry and the 2014 version of the state voter registry](#) can be found in the illegally traded datasets.

While the general public has not been bothered by such “revelations” beyond receiving unsolicited mass SMS advertising, many state databases contain potentially sensitive personal and commercial information. The recent [incident in Novi Sanzhary](#) demonstrates how unsolicited access to thousands of telephone numbers of residents of a particular territory may be used to disseminate disinformation, instigate mass panic, and provoke unrest through the massively popular messenger app Viber and other social networks.

## 5.3. Semi-legal or illegal sources

Additionally, Ukrainian legislation does not explicitly prohibit **combining personal data on citizens from various open sources**, including, for example, government registries available through [open data regulations](#), job seeker databases, and social networks. Enterprises have appeared that offer all supposedly publicly available data about physical persons or entities, or provide the “service” of combining separate pieces of data.

A Telegram bot @info\_baza developed in 2019 ties a telephone number to a person’s name or vice versa and searches for other personal data associated with an email, a photo of a person’s face, or a car plate (Image 38). The bot does it for free or in exchange for another telephone

number (or several) from a user's phonebook (expectedly, without requesting consent of the owner), while a larger dataset requires a modest payment of 50 US dollars. The creators of the bot, whose identity remains undisclosed, insist their original data was collected from open job seeker websites, but there are indicators some of it [may have also come from leaked consumer databases](#). It is also not inconceivable that instead of leaking the whole databases, active [employees of state bodies](#) or [private enterprises](#) could sell bits and pieces of data they have been authorized to access on the side, as in cases previously uncovered by Ukraine's law enforcement authorities.

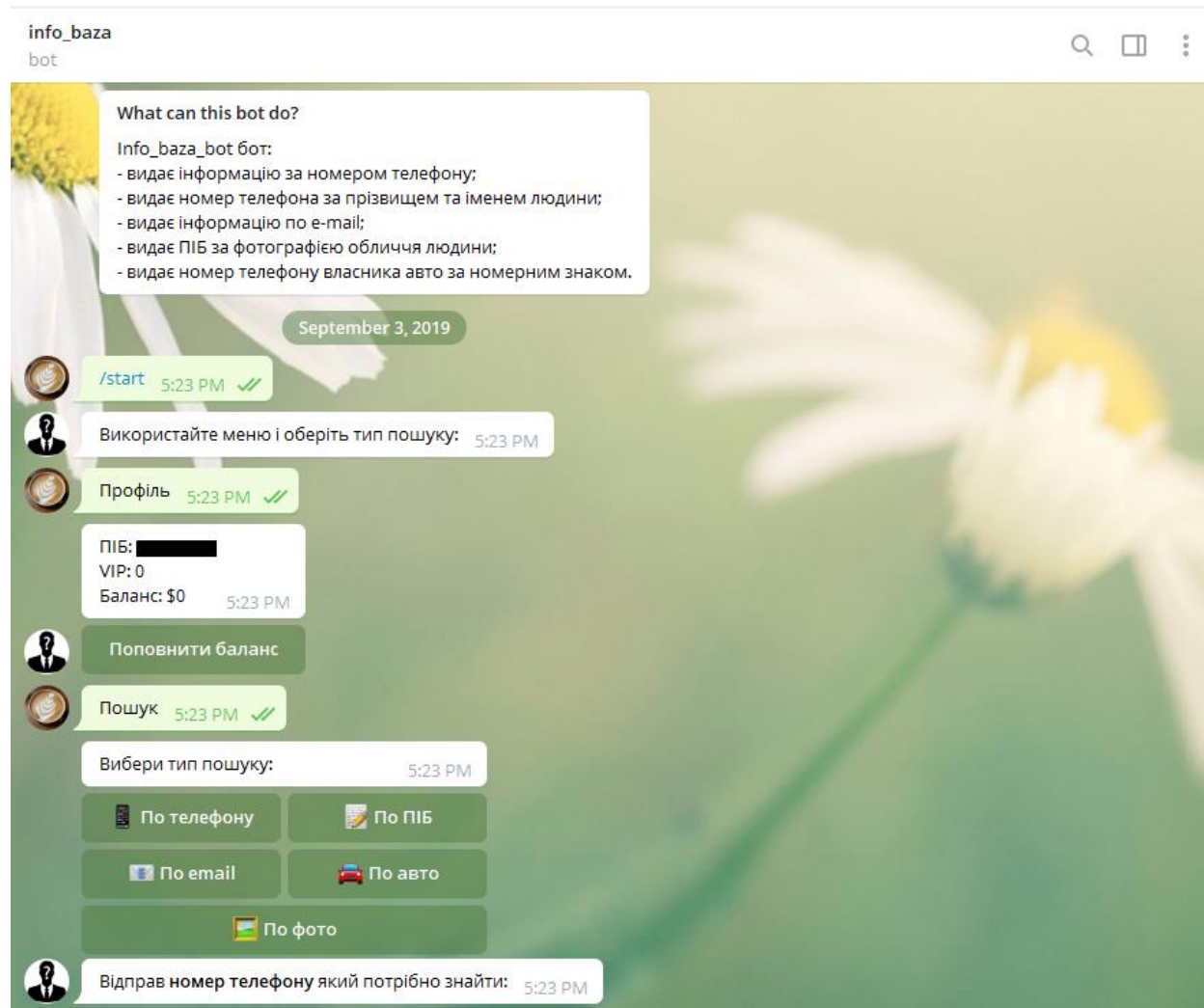


Image 38. Possible data request options from @Info\_baza Telegram bot. Screenshot 03.09.2019

At the time of writing this report, another anonymously created Telegram bot called @UA\_Baza appeared, offering even more detailed information about millions of citizens for sale, including such sensitive details as [passport numbers, personal identification codes, declared places of residence, social media passwords, and even bank details](#). This list indicates that such data could not have been collected from sources openly available online (Image 39). Moreover, the

bot directed users to detailed instructions on how to purchase data with Bitcoin payments equivalent to 50 US dollars per 10 records.

After a public outcry and an [official investigation](#) about sensitive citizen data being leaked on the Internet, the original bot was disabled but later reappeared online under multiple names. The investigation concluded that the data had been taken from various datasets. A journalistic investigation [suggested](#) that it combined data from government registries, commercial databases, and social media. Given the nature of such leaks, it is quite impossible to predict where the database will resurface next or how it might be used in the future.

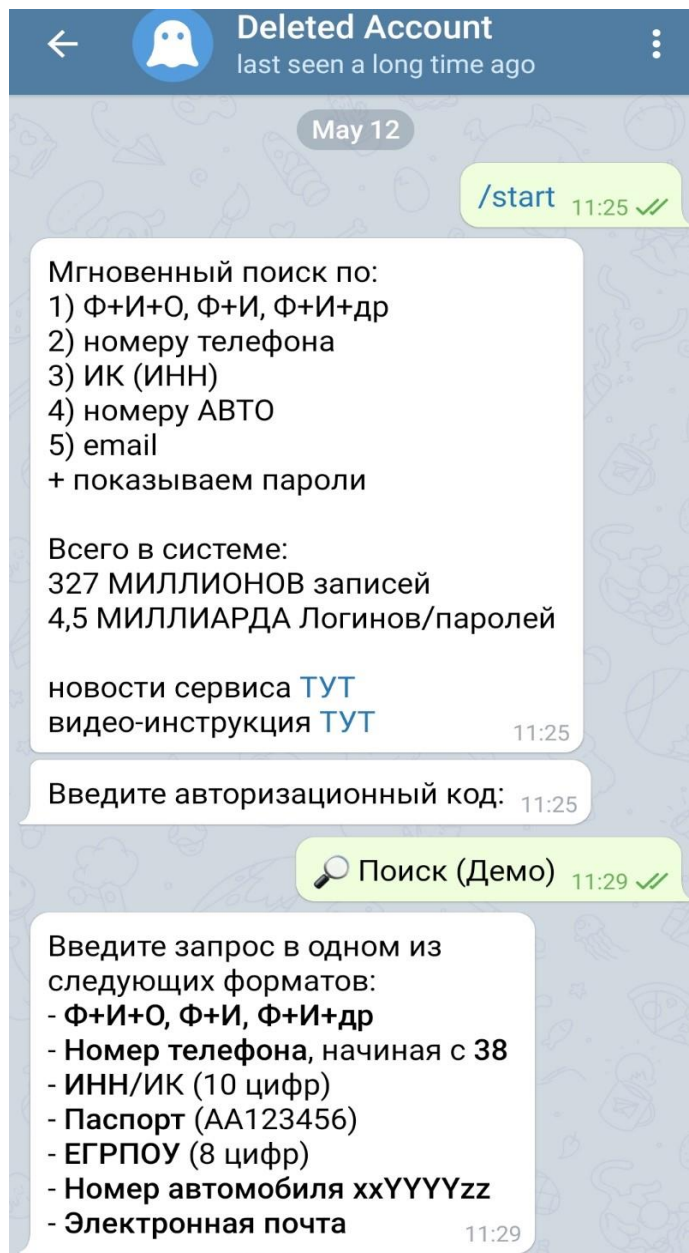


Image 39. Possible data request options from @UA\_baza Telegram bot, including sensitive personal data such as a passport number or personal tax number. Screenshot 12.05.2020, account disabled the same day.

## 5.4. Consumer data

Several commercial companies in Ukraine maintain very large consumer databases, including [online retailers](#), telecommunication companies, [banks](#), and [logistic operators](#) that mostly collect consumer data for their own purposes while sometimes offering third parties an option of advertising to their clients. In addition, several nationwide loyalty programs — some including a [network of over 90 online stores](#) — and millions of clients exist across Ukraine. Additionally, [digital advertising networks](#) operate their own data management platforms that collect and analyze websites' traffic, including user data, and use real-time bidding to sell targeted ads. Smaller businesses also operate client databases. While large consumer datasets sometimes become available for sale online through hacks or leaks from dishonest employees, smaller businesses frequently sell their client databases.

Technically, selling consumer data without the informed consent of such consumers is illegal under the Law on Protection of Personal Data. However, Ukraine lacks effective regulations and mechanisms for holding such traders accountable.

## 5.5. Plausible sources of voter data in the 2019 political campaigning

While not impossible, we have not come across any indication that political parties have been using consumer databases for their campaigning or attempted to purchase such. In turn, parties appear to have relied on their own membership list as well as data collected from their prospective voters and activists, even before elections. While our report focuses on online data collection methods, there are indications that election contestants have also collected personal data offline, with election watchdogs reporting instances of parties and candidates doing so [under false pretenses](#) or violating the [principle of informed consent](#). Media reports indicate that some parties [shared the databases of supporters formed during the 2019 Presidential elections](#) with their Parliamentary candidates.

As described earlier in this report, some parties, like the Servant of the People or European Solidarity, have managed to collect information about tens of thousands of voters online and segment them into rather detailed categories according to demographic or behavioral characteristics. According to a digital marketing consultant that worked with 2019 election contestants interviewed for this report, a solid initial list of target voters combined with Google or Facebook's targeting capabilities, for example, through such functions as Facebook's "[Lookalike Audiences](#)" would be enough for a party to build a competitive digital campaign in Ukrainian realities, even though the data on the users of these platforms in Ukraine is not as granular as, for example, it is in the US.

## 6. Considerations of pre- and post-election data ownership and sharing

### 6.1. Party-affiliated projects

Both before and during elections, some of the parties spun off affiliated projects targeting a wider circle of active citizens that may share parties' political goals yet not be ready to formally join the ranks of a political organization. For instance, a few years ago **European Solidarity** started a joint project with IDF Reforms Lab, launching the so-called "Open Office" to engage citizens ready to help "[form of a new political culture and implement qualitative reforms on all levels](#)". In 2019, **Holos** invited its most active volunteers and supporters to join "Co-workings for change" in several regions, and a newly elected President Zelensky announced the launch of "Lift," a project to help engage talented individuals who wanted to contribute their ideas or skills to "[positive changes in the country and its comprehensive socio-economic and cultural development](#)."

While the publications on the website of the "Open Office" of European Solidarity do not indicate any activity since 2018 (albeit there's a working registration form), and Holos [used its regional "co-workings" for organizing party volunteers](#) during the campaign, the relationship between Lift and Servant of the People was more convoluted. The [description on the website](#) implies that the project is an attempt by the new President and government to recruit qualified people as public servants and solicit ideas for the improvement of government services in an efficient and transparent manner. In fact, currently users may apply for a position in a state body, leave an unsolicited application with general information about themselves and a CV, or propose a product for digitizing government services. While the website has a privacy policy and asks users to consent to processing of their data, nowhere does it explain the exact relationship between the platform, the party, and the government bodies or how the data transfers are handled between Lift and such third parties (in fact, the privacy policy only states that the website administrator would contact a user when requesting personal information for purposes beyond those already listed, which do not include data transfers to state bodies, for instance). This unclear connection prompted some confusion among Servant's supporters during the campaign period, with many using the website to apply to join party ranks only to learn that their applications were invalid (Image 40). At the same time, upon launching the platform, the head of Servant's campaign headquarters implied that the project could be used for scouting candidates to run in the upcoming elections.

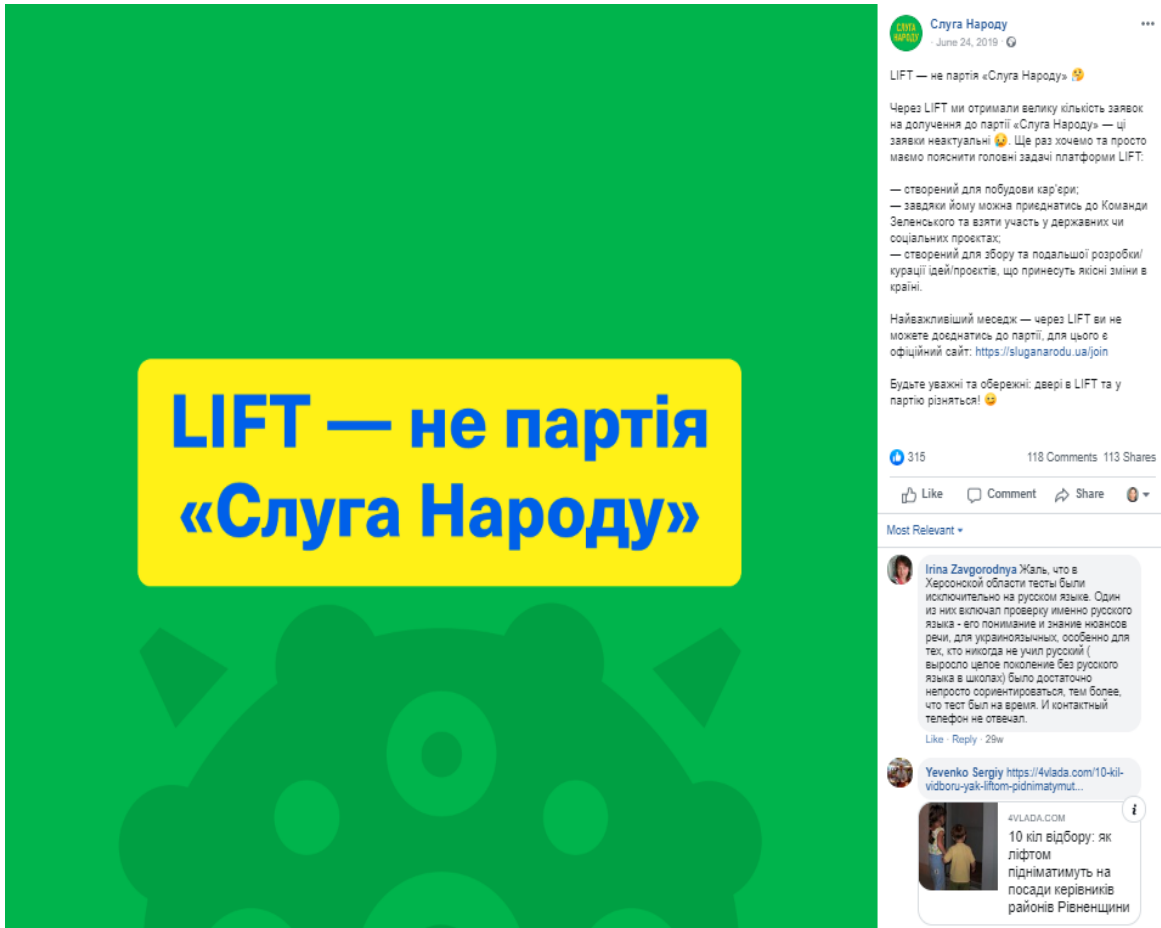


Image 40: 24 June, 2019, Servant of the People Facebook post explaining how to join the party via its website and not the LIFT initiative, screenshot 19.03.2020

## 6.2. Government entities and elected representatives

For parties and candidates that win an election, voter data collected during the campaign becomes their constituent data. Handling such data in a new capacity deserves careful consideration. Thus, even if the voters consented to their data being used by the party or the candidate beyond an election cycle, they may not expect it to end up in the hands of a government official or be shared with or used by a state body. Even if the elected representatives do not technically own the data (i.e., subscribers on a social media platform) but “inherit” it from the party that ran them as candidates, same considerations should be taken into account.

Nevertheless, Facebook’s Page transparency record indicates that after the Presidential elections of 2019, the new administrators of the Presidential administration’s Facebook page simply merged it with the page of Volodymyr Zelenskyy’s supporters (Image 41), leaving his [180,000 subscribers](#) no choice of whether or not to follow the new administration’s page.

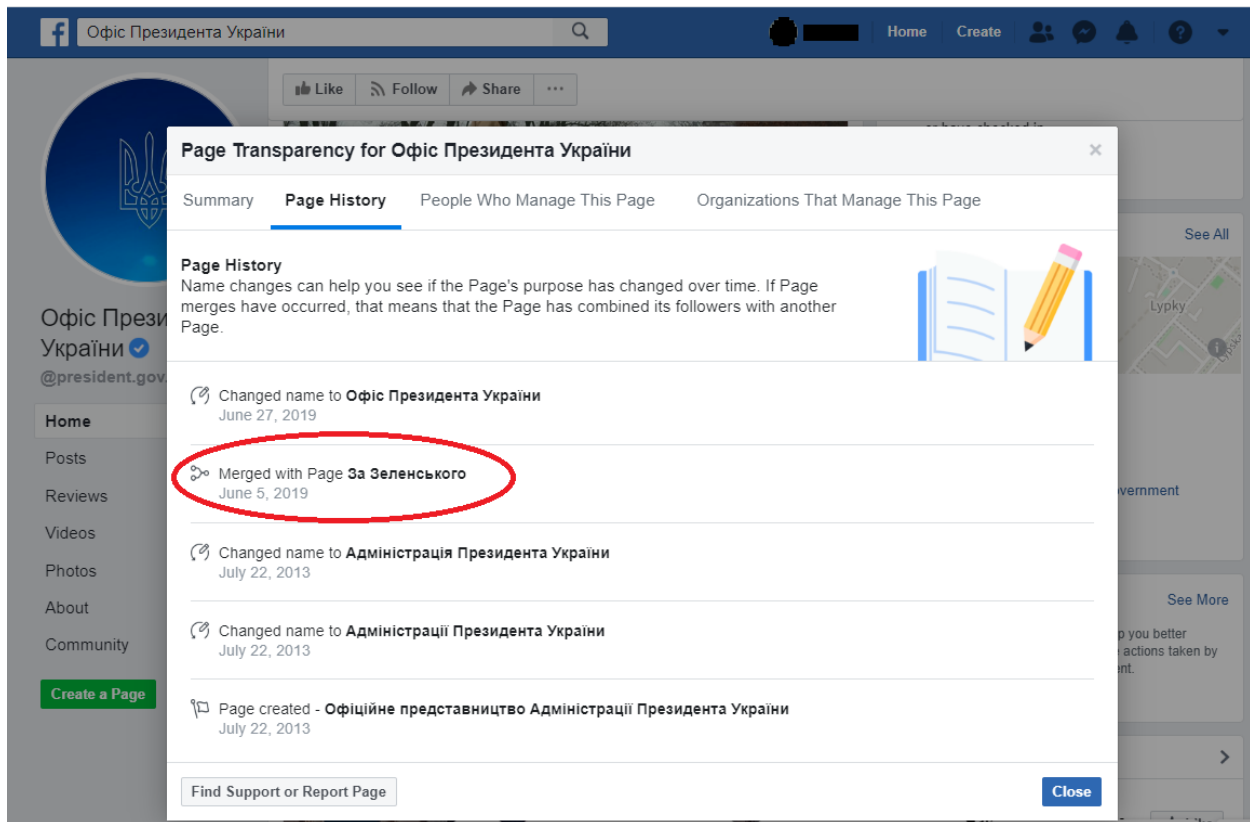


Image 41: A screenshot of Presidential Administration's Facebook page history showing a merge with Zelensky's campaign fan page after elections, screenshot 9.03.2020

Additionally, in November of 2019, the founder of one of the leading digital marketing agencies in Ukraine [posted](#) a screenshot from an email message by the newly created Ministry of Digital Transformation, claiming that he had begun receiving such communication to a single-use email address he created especially to subscribe to e-mails from Zelensky's election campaign (Image 42).



**Maksym Savanevskyi**

November 4, 2019 · 🌐

От прям прекрасно. Маю звичку при реєстрації вказувати одноразові імейли, щоб можна було відслідкувати, як ті, кому передав свої дані, потім юзують їх.

Залишив я один імейлик на сайті Зеленського під час передвиборчої кампанії. А тепер на цей імейлик мені прийшов лист від Мінцифри.

Тобто штаб Зеленського передав імейли в Мінцифру. Прекрасно ж. Не?

Мінцифра - це про цифрові послуги. Цифрові послуги - це дуже багато про персональні дані.

Персональні дані - це те, що в тому числі й Мінцифра, мають якимось чином оберігати.

**- Хей, Мінцифра, а ви щось чули про захист персональних даних?**

**- Ніт, не чули**

Мінцифра <hello@e.gov.ua>

📧 Дайджест: 4G у регіонах, е-права та центр розвитку стартапів



Міністерство  
цифрової трансформації  
України

**Привіт, це команда Мінцифри!**

Ми активно працюємо та хочемо, щоб громадяни знали, що відбувається в Міністерстві та як проходить робота над проєктами. Тому вирішили ділитися не тільки новинами, а й маленькими перемогами та поразками.

Image 42: A November 4, 2019, Facebook post by a voter sharing a screenshot of an email message from the newly created Ministry of Digital Transformation, allegedly sent to a single-use email address he created specifically to subscribe to e-mails from Zelensky's election campaign. Screenshot 10.05.2020.

## 7. Conclusions

This report attempts to contribute to the growing body of research on the impact of technologies that leverage personal data for political campaigns by investigating the treatment of voter data by five political parties during the 2019 Parliamentary elections in Ukraine. In order to answer important questions about the implications of such technologies for voters, political actors, policy makers, and the democratic process itself, it is necessary to understand whether and how these

technologies are being applied in different countries and their impact on the political process in particular political, legal, and social contexts. Such research is especially important in light of rapidly evolving technology and the increasing utilization of approaches developed by the commercial data industry for political means, and not just by the traditional political players, but by the variety of other actors and outside the boundaries of traditional electoral cycles.

Based on the findings of our research, we identify several important questions and recommendations that should be considered by **political parties, regulators, and civil society**. We hope our conclusions will help fuel an important discussion within Ukraine and inspire researchers to undertake similar studies in other countries of this region and beyond.

- Rapid development and proliferation of technologies that utilize personal data for political purposes translates into regulations lagging behind and new tools being applied largely in a legal vacuum. This situation is exacerbated by society being unable to fully understand what technology is used by political actors during the campaign and to what end. In these circumstances, it is important for political parties to think beyond merely meeting legal requirements but consider aligning their political practices with their ethos. It is also important to be thoughtful and transparent about the use of voter data, including any data shares with third parties. At a bare minimum, parties should formulate clear data protection/privacy policies, display them on all campaigning platforms, and ensure voters' consent is given before any data is collected from them. It would be laudable for the parties to accompany their data protection practices with an explanation of what they are doing to ensure the security of the voter data parties are holding.
- Where privacy policies are in place, parties need to clarify how those translate into practical application with regard to a variety of tools utilized for digital outreach and ensure that appropriate campaign members are aware of these directives and that they are consistently applied at every level of the campaign's organizational structure.
- We found that the security of digital platforms and tools used during an election campaign has often been an afterthought. While not all parties enjoy equal resources during a campaign, this aspect should be prioritized and appropriate measures should be taken to protect voters' personal data. As demonstrated by such examples as the 2016 USA election, a breach of security may have far-reaching negative consequences not just for the party itself or the voters if their data is compromised, but could impact the election outcome and even cause society to question the legitimacy of the overall electoral process.
- Voters' data collected by political parties does not just magically disappear after an election, nor does it lose its value. For the parties that win an election, voter data turns into constituent data, which should be treated with special consideration. When voters consent to their data being used by the party beyond an electoral cycle, they may not expect it to end up in the hands of a government official or be shared with or used by an official state body. Nor should this happen automatically, even in cases when the party in

question receives overwhelming voter support and leads the formation of the government. Therefore, it is important to make post-election data processing and sharing mechanisms as transparent and understandable to voters as possible, as this may impact their level of trust to the government and the overall political system.

- Ukrainian lawmakers and electoral administration are keen on introducing such innovations as e-voting technology, yet existing legislation still lacks important clarifications, mechanisms, and safeguards pertaining to digital campaigning and protection of voters' personal data. At minimum, the legislation should recognize digital campaigning, including but not limited to online political advertising, as a form of electoral campaigning and pay special attention to such emergent issues as proliferation of discrediting or misleading campaigning online, the role of pages not officially affiliated with political contenders, or usage of bots and fake accounts. In addition, election administrators must provide clear mechanisms for reporting funds spent on digital campaigning activities by political parties and candidates, thus establishing grounds for holding those breaking the rules accountable.
- Any additional digital campaigning regulations, if passed, should not threaten the freedom of speech online. Moreover, online platforms are making increasing efforts to increase transparency and accountability around digital political advertising and adjust their practices according to election laws. Ukraine should try to coordinate with tech giants on a state level to ensure its electoral legislation is also followed by the companies operating internationally.
- Personal data related to citizens' political beliefs and memberships in political organizations is already considered to be "sensitive" by Ukrainian law, which calls for enhanced safeguards of such information. And while the parties collecting data on their members seem to be exempt from submitting respective notifications to the Ombudsman's office, existing directives do not specify what should be done about the data of non-members, such as volunteers, supporters, and other voters, collected by the political parties and candidates during election campaigns. Moreover, it is doubtful whether the mechanisms meant to provide such safeguards are effective in the first place given that Ukraine does not have a separate data protection body with sufficient authority and resources to enforce regulations.
- Additionally, the law implicitly requires political parties to ensure the security of their websites, which would realistically prevent voters' data from being intercepted or lost. Yet there is no clarification on what providing such security for a website or another digital tool entails. And while such prescriptions are best excluded from the law, political parties and other players involved in political campaigns would benefit from clear guidance on citizens' personal data protection in elections as well as effective mechanisms for enforcement of such measures. The Ukrainian civil society could take it upon itself to formulate such guidelines.

- A related yet even more alarming issue is the absence of a culture of privacy and low awareness of associated risks among regular citizens, private entities, and public authorities. The volume of citizens' personal data already available online as a consequence of leaks, hacks, or illegal trade creates ripe conditions for targeting vast numbers of citizens with any potentially malicious content and could be exploited by both domestic and external actors in a variety of contexts, including political. In the face of such imminent threats, Ukraine should prioritize strengthening its data protection mechanisms, while civil society could work on raising public awareness about the importance of privacy.
- At the same time, proliferation of increasingly sophisticated and non-transparent technology used in political campaigning leaves voters dumbfounded and could contribute to the perception of being manipulated. Civil society in Ukraine should invest in increasing the digital literacy of voters and demand transparency of the mechanisms used for digital campaigning, all the while being conscious of not causing society to lose faith in political parties and the overall electoral process.