

**Title:** Poster: Understanding the Privacy Practices of Political Campaigns: A Perspective from the 2020 US Election Websites

**Authors:** Kaushal Kafle\*, Prianka Mandal\*, Kapil Singh†, Benjamin Andow§, and Adwait Nadkarni\*

**Author Affiliations:** \* - William & Mary, † - IBM T.J. Watson Research Center, § - Google (work completed at IBM Research)

**Venue:** 45th IEEE Symposium on Security and Privacy (S&P)

**Date:** May, 2024

**Paper DOI and Link:** <https://doi.ieeecomputersociety.org/10.1109/SP54263.2024.00091>

**Abstract:**

Political campaigns are known to collect private user data, whether for building voter profiles, engaging with volunteers, or for soliciting donations. However, as such campaigns are classified as nonprofit in the United States (U.S.), their privacy practices have not received the same level of scrutiny as those of for-profit enterprises. This paper presents the Polityzer framework to evaluate the privacy posture of political campaign websites, and uses it to analyze 2060 campaign websites active during the U.S. election of November 2020. Our analysis leads to 20 key findings that demonstrate gaps in the privacy postures of political campaigns. For instance, we find that campaigns collect extensive private data they are not required to by the Federal Election Commission (FEC), and a vast majority do not provide any form of privacy disclosure. When disclosures are provided, they are often incomplete. We also found that campaigns may be inadvertently sharing data with other campaigns through common fundraising platforms, without disclosing such sharing. Reporting the lack of privacy disclosure to the respective campaigns yields further insights into the rationale behind their security posture. Finally, we discuss ways in which our results could enable future research, inform emerging privacy regulations, and transform user behavior regarding data privacy in this critical context.

# Understanding the Privacy Practices of Political Campaigns: A Perspective from the 2020 US Election Websites

## Motivation

- Election campaigns collect large volumes of data from various sources for voter profiling.
- They also do so to comply with donor disclosure regulation enforced by the Federal Election Commission (FEC).
- However, as non-profits, they are not regulated under any data privacy laws (e.g. CCPA).

## Methodology

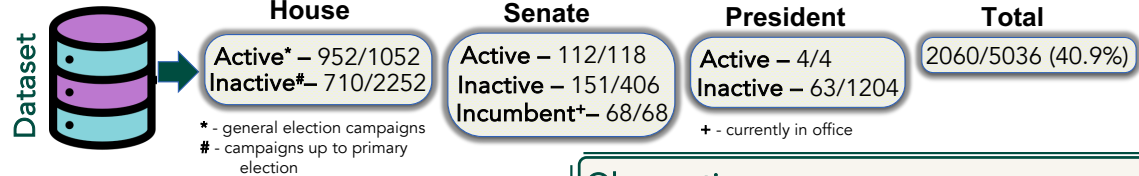
- Collect candidates from FEC database.
  - Find candidate's Ballotpedia profile using search attributes like name and state.
  - Extract candidate's web URL and save their website to our local database using a website crawler.
  - Extract data types collected by each website, their privacy policies, URLs for further analysis.
  - Analyze the security and privacy practices and aggregate results.
- ✔ Fully automated    ✔ Semi-automated

## Security Findings

687/1504 (45.7%) have trackers but no privacy policy.

168 (8.2%) did not use HTTPS, 86 of which collect PII.

38 websites were hosted outside the U.S.



## Data Collection Findings

1462 (70.97%) collected Personally Identifiable Information (PIIs).

12 collected PII of parents or friends. 2 collected PII of user's partner.

61 (2.96%) collected socio-economic opinions with PII, linking individuals to political leanings.

Email/name, phone and location were the most collected data types.

## Privacy Policy Findings

1499 (72.77%) did not have a privacy disclosure. 968 (64.58%) of them collect PII.

222/493 (45.03%) did not fully disclose all PII in their privacy policy

Campaigns may be inadvertently sharing data due to privacy policy conflict with fundraising platform.

None discuss what happens to data after campaign concludes.

3/26 campaigns we signed up in shared our email address without a privacy policy.

## Observations

- Current lawmakers (144 election winners, 9 incumbents) did not have a website privacy policy.
- 56/153 (36.6%) of the lawmakers serve in privacy-related committees, which help formulate privacy laws.

## Campaign Responses

- We received 20 wide-ranging responses during our finding disclosure.
- Reasons for not having a privacy policy included lack of expertise, campaign no longer being active (although the website still was), and a lack of federal law asking for one, with one candidate even asking us to convince their party for change.
- Campaigns also asked us for privacy policy templates in their responses, revealing a lack of resources and technical know-how.

## Lessons

- Proper disclosure of data collection/sharing required to inform users how their data is used.
- Voter data is vulnerable to current and future exploits, as no campaign discusses what happens to collected data once campaign concludes.
- Campaigns must allocate resources to enhance their privacy practices.

**Authors:** Kaushal Kafle<sup>1@</sup>, Prianka Mandal<sup>1</sup>, Kapil Singh<sup>2</sup>, Benjamin Andow<sup>3</sup>, Adwait Nadkarni<sup>1</sup>

**Affiliation:** 1 – William & Mary, 2 – IBM Research, 3 – Google

**Contact:** @ – kkafle@wm.edu

