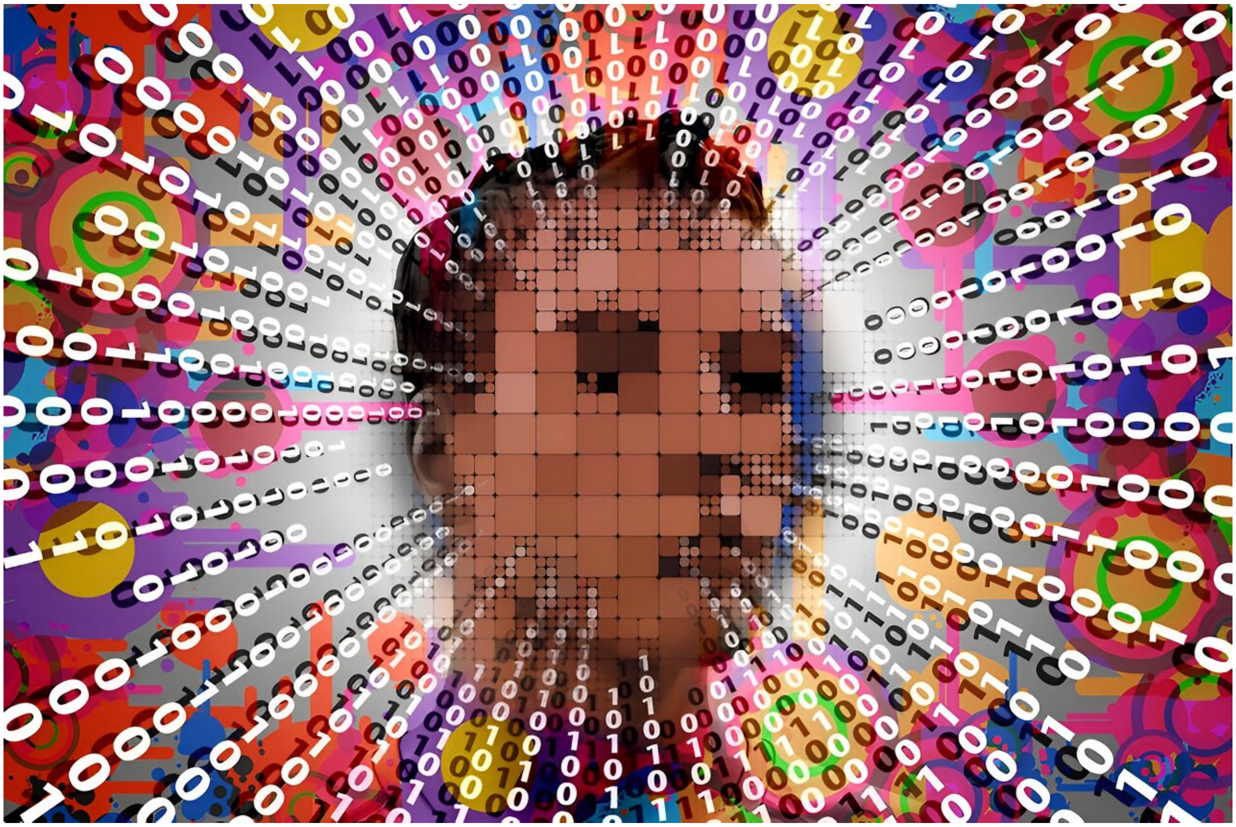
Your personal data is political: Computer scientists find gaps in the privacy practices of campaign websites

February 7 2024, by Antonella Di Marzio



According to researchers from the Secure Platforms Lab, data privacy is a bipartisan issue and regulations are needed to prevent political campaigns from misusing user data. Credit: Gerd Altmann from Pixabay

Would you trust a random political canvasser to do whatever they wanted with your resume, your friends' email addresses—and perhaps your profile pictures?

That's precisely what you may be doing when interacting with political campaign websites, according to a new study published in the *IEEE Symposium on Security and Privacy (SP)* by researchers from William & Mary, Google, and IBM. Two W&M doctoral students in computer science—Kaushal Kafle and Prianka Mandal—respectively served as first and second authors.

The underlying research has already been presented at many events—including the 2023 Commonwealth Cyber Initiative Symposium, where it won the Best Poster Award.

"The only thing users can really do to keep their data safe is to not provide it in the first place," said co-author Adwait Nadkarni, Class of 1953 Associate Professor of Computer Science and Secure Platforms Lab lead at William & Mary.

The study examined 2,060 House, Senate, and presidential campaigns from the 2020 United States election cycle, representing the first large-scale analysis of the privacy practices of political campaign websites. Those campaigns, the study revealed, often retained extensive private data for an unspecified amount of time, generally provided incomplete or no privacy disclosures, and were likely to share data with other campaigns or sell them post-election.

Highly private data was often collected alongside contact information, the study found, allowing campaigns to build user profiles without their explicit consent. The often undisclosed use of trackers gave campaigns access to user browsing habits, exposing them to microtargeted political ads that have often been defined as manipulative and as a potential danger to democracy.

Nadkarni remarked that this work "just happened to fit" with the data and democracy initiatives from the university's Vision 2026 strategic plan, as well as the proposed new school in Computer Science, Data Science, Applied Science, and Physics. The research process also highlights another Vision 2026 pillar—careers.

"This paper came out of an existing collaboration with IBM Research," said Nadkarni. "The way these collaborations usually work is having students intern with collaborators, working on collaborative research as part of their internship project."

What data are we surrendering?

Political campaigns, Nadkarni explained, are classed as nonprofit, receiving less scrutiny than commercial enterprises. They collect data of significant value but still aren't subject to the same regulations applying to businesses.

Over two-thirds of the 2,060 campaigns examined were found to collect personal information through their websites, with the most collected data being email addresses (99%) and phone numbers (62%). Other data types ranged from political opinions to social media information and, in rare cases, data such as union status and race, defined as "highly sensitive" by the researchers.

A few campaigns also obtained information about people other than the user—thus without consent.

The researchers performed two additional studies to understand data-sharing implications. Thirty-one percent of campaigns shared email information with other political entities, but over one-third of these didn't mention data sharing in their privacy policy. Sixty-one percent of campaigns using fundraising platforms did not have a privacy policy at all.

None of the campaigns disclosed how long they would retain user data. "So, what happens to that data after the campaign ends? You should accept that it is going to remain there in perpetuity," said Kafle.

Researchers also conducted a security risk analysis and found out that campaign websites were generally secure, although a small number included malicious outbound links that weren't adequately vetted. Seventy-three percent of campaigns used trackers. Of these, almost two-thirds didn't have a privacy policy; among those that did, one in four did not mention trackers.

Privacy as a bipartisan issue

The study did not disclose or discuss the political affiliations of candidates. However, its dataset remains open in order to enable future research.

"Privacy really is a bipartisan issue," said Nadkarni. "We didn't want the message to become 'this particular party isn't doing privacy right,' but rather 'there needs to be a legislation to actually make everybody follow best-practice guidelines.'"

Retaining data in perpetuity does not only represent a privacy issue, the study argued, but also a security problem due to the potential for data leaks. All campaigns come to an end, but their URLs and the associated user data can be bought by offshore entities for potential malicious use.

Previous studies and news articles, the researchers said, had indicated it was not uncommon for candidates to switch party affiliation after their campaigns. "If you had donated to their campaigns, you may not agree with their current position, but your data still remains with them," said Nadkarni.

Users, Nadkarni remarked, are not currently in control. The only immediate countermeasure is not volunteering information, especially about third parties, and sharing the bare minimum of data required when donating to a campaign.

"But what users can do in the long term is ask their lawmakers to make regulations to prevent campaigns from misusing data," he said. "Just like there have been movements to rein in for-profits and their use of information, there needs to be a similar push for regulating political campaigns."

The Voter Privacy Act Bill introduced in the Senate, which follows the blueprint of the European Union's General Data Protection Regulation, represents an effort in this direction.

The researchers also reached out to campaigns directly, which opened to some positive interactions. Many campaigns, being grassroots-run, didn't have the technical expertise to protect the data; Nadkarni said that further research will be looking at examples of "good" campaigns to offer a good blueprint of how to safeguard privacy in the political campaign space.

The research team will also be looking at campaigns from the upcoming 2024 federal elections, having already analyzed campaigns from the 2023 Virginia elections.

Kafle said that their paper aimed to raise awareness of how non-profit entities were processing data. He said that their poster had already attracted considerable interest at different venues.

"I think almost everyone perceived this to be a bad situation, but to be staring at that in numbers was something else," he said. "We intend to increase public attention and awareness on this topic as one the key outcomes of this study."

More information: Kaushal Kafle et al, Understanding the Privacy Practices of Political Campaigns: A Perspective from the 2020 US Election Websites, *IEEE Symposium on Security and Privacy (SP)* (204), DOI: 10.1109/SP54263.2024.00091. www.computer.org/csdl/proceedi … 3000a091/1Ub22Yc2aOc

Provided by William & Mary

Citation: Your personal data is political: Computer scientists find gaps in the privacy practices of campaign websites (2024, February 7) retrieved 6 May 2024 from https://techxplore.com/news/2024-02-personal-political-scientists-gaps-privacy.html