

Algorithms seek out voter fraud

November 5 2019, by Whitney Clavin



Credit: CC0 Public Domain



Concerns over voter fraud have surged in recent years, especially after federal officials reported that Russian hackers attempted to access voter records in the 2016 presidential election. Administrative voting errors have been reported, too; for example, an audit by state officials revealed that 84,000 voter records were inadvertently duplicated by the California Department of Motor Vehicles (DMV) in the 2018 June primary election.

Michael Alvarez, professor of political science at Caltech, and his team are helping with the situation by developing <u>new algorithms</u> for tracking <u>voter</u> data. They have partnered with Neal Kelley, Orange County's registrar of voters, and, from April 2018 to May 2019, evaluated more than 1.5 million voting records in Orange County. The project's first results, reported in the journal *American Politics Research*, show that this type of technology can be used to assess the integrity of an election. In this case, however, no instances of fraud or significant administrative errors were found.

"Manipulations to voter records can wreak havoc on an <u>election</u>," says Alvarez, who also works on the larger Caltech/MIT Voting Technology Project, formed in the aftermath of the controversial 2000 <u>presidential</u> <u>election</u>. "You could have people showing up to vote who are not on the list, or people's addresses can be changed in the databases so that voters do not get their instructions in the mail. There are many scenarios, some fraudulent and some administrative, that can negatively influence the quality and integrity of elections."

The team's algorithms are designed to take snapshots of voting records on a daily basis. Even without any fraud or errors, voting records are constantly changing due to the addition and removal of voters, changes in addresses and other administrative processes. Alvarez and his team,



led by Caltech graduate student Seo-young Silvia Kim, developed one algorithm to measure the dynamic changes taking place in voting records and a second algorithm to look for statistical anomalies in that dynamic process.

"We want to make sure that the changes we are seeing are expected and not unwanted," says Kim, a social sciences PhD candidate with a focus on political science, who learned computer programming skills on her own while working on this project. "Are there any obvious red flags?"

"Orange County is a great laboratory for this study," says Alvarez. "Neal Kelley is very dedicated to this process, and we have built a strong collaboration with Orange County."

A third algorithm developed by the team scans for duplicates of voting records. Duplicates are a normal occurrence in voter databases that arise, for example, when voters move or register at multiple places, but they can also indicate malfeasance or errors.

"Monitoring for duplicates is an indicator of the health of a voter database," says Spencer Schneider, a Caltech sophomore who worked on the project as a Summer Undergraduate Research Fellow (SURF) student and who is the second author of the paper.

The team says one goal of the project is to share what they are learning with the public so that others can monitor voting records and political scientists can access the data for their research. To that end, the team has posted their results and computer codes online. They have also begun a similar project with Los Angeles County; in Oregon, they are monitoring votes that come in by mail.

"Administrative errors and the potential for shenanigans loom large in U.S. elections, and we need to fend off possible corruptions to voter rolls



in a timely manner," says Alvarez. "Our vision is to have all states upload voter data on a daily basis and to have algorithms monitor their integrity."

Provided by California Institute of Technology

Citation: Algorithms seek out voter fraud (2019, November 5) retrieved 2 May 2024 from <u>https://phys.org/news/2019-11-algorithms-voter-fraud.html</u>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.