A Voter's Guide to Data Privacy

Who you vote for is still private. Almost everything else is not.

How do they get information about me?

"We don't just have the information they're tweeting about, we can match them with their voting and purchasing habits in order to target them through email and social networks"

—Jesse Kamzol, Chief Data Officer for the RNC

- **Voter Registration Lists** (public in many states)

- **Other Public records** (tax assessor, census, change of address records, marriage, arrest and court records, motor vehicle, professional and business licenses, campaign donor rolls, SS for records of the deceased)

- **Consumer behavior** (online and in person shopping, loyalty/discount cards)

- **Location data** (from google, from apps, from your device)

- **Data you give away** (online/phone surveys, any time you sign up for something, letters to newspapers, online comments)

- **Social Media use** (profile, comments, likes, tagging people, "signing in" to apps with FB, profile picture)

- **Television** (TV set top boxes collect and share data about what you watch)

- **Browsers and search engines** (cookies, trackers)

- **Phones** (apps and app permissions, location, browsing, geofences)

- **Campaigns** (donation and volunteer lists, from door-to-door and phone canvassers, from apps and newsletters you sign up for)

Who has the information about me?

"Instantly download the files you need from our National Voter List of 213+ million voters, National Donor List with 137+ million donations and our New Mover list of 17+ million monthly movers."

—Aristotle.com, Campaign Manager Software

Commercial Marketing Services (Acxiom, Dun & Bradstreet, InfoUSA, Experian, Epsilon, Sprinklr, Dstillery)

Political Data Consultants (i360, Aristotle)

The GOP Data Center (Republican Party)

NGP VAN (Democratic Party)

These each have:
- large databases of registered voters
- up to 2,500 pieces of data about voters in each one
- ability to segment lists into small groups of voters who think alike

Voter registration lists include:
- voter name, email, address, phone number, date of birth, voter ID#, party affiliation, gender, race, and more
- each state decides which items are public; Federal Law, the 2002 HAVA, requires states maintain a digital list of voters but does not require the list remain private

Learn More: Big Data, Artificial Intelligence, & Political Profiles

Big Data and AI make it possible for all this data about registered voters to be collected and then aggregated, or combined, into very large databases that connect each voter to the data about them. The thousands of pieces of information about us are used to create political profiles and scores for each of us that predict our voting behavior. And those are in turn used for microtargeted advertising (see next page).

Learn More: https://policyreview.info/articles/analysis/digital-commercialisation-us-politics-2020-and-beyond

A Voter's Guide to Data Privacy

Who you vote for is still private. Almost everything else is not.

Why is voter privacy important?

"Political dossiers may be the largest, unregulated assemblage of personal data in contemporary American life."

—Ira S. Rubinstein , senior fellow at the NYU Information Law Institute

Lack of individual control or ability to opt out
- We don't know what information they have about us, how they are using it, or what our political profile "scores" are
- We don't have the option to opt out though it might be possible to opt out of each company's software, for example: https://brandyourself.com/blog/privacy/acxiom-opt-out-and-removal/

Insecurity/Breaches of data
- the list of voter data breaches is long
- Anyone needing extra privacy, like a stalking victim, is vulnerable

Secondary use of our data
- This is when you sign up for a service but your info is being sold to others
- In 2016, each Republican candidate gave their donor lists to other candidates

Microtargeted Advertising
- Advertising that is directed a small segments of people who think alike
- Both major parties use microtargeting. In 2016, the Trump campaign microtargeted registered voters to stay home & not vote

What can I do to protect my privacy?

"Privacy shouldn't be a matter of personal responsibility. . . Privacy should be a right, not a privilege . . . Everyone deserves to live in a world—online and offline—that respects their privacy."

—Electronic Frontier Foundation

1. **Learn more about microtargeting!** https://whotargets.me/en/
2. **Campaign for (stronger) voter privacy laws**
3. **Renovate your social media profile**
   (Stop using social media apps [use a browser], review privacy settings, clear activity logs, stop tagging people, never use "sign in" with social media)
4. **Clear your location** from apps, google, and your phone/tablet
5. **Stop giving out your information!**
   (stop taking online surveys, use a separate email to sign up for services, rewards cards, political apps, newletters, etc)
6. **Spring clean your phone**
   (delete apps you don't use, limit app permissions, clear location history)
7. **Limit online tracking:**
   - Use privacy focused browsers (FireFox, Brave, Duck Duck Go, TOR)
   - Use privacy focused search engines (DuckDuckGo, Qwant)
   - Block trackers with browser extensions (Privacy Badger, uBlock Origin)
   - Encrypt online connections (HTTPS Everywhere)
   - Consider using a Virtual Private Network (VPN)
   - Check to see if you are being tracked: https://panopticlick.eff.org/

Learn More: Legislation

There is no federal legislation to protect this data about us or to make voter registration lists private. Each state has its own laws and only California has passed a law protecting data privacy; the California Consumer Privacy Act (CCPA). There is a bill, held up in the senate, called the Voter Privacy Act.

Learn more about the Voter Privacy Act here: https://epic.org/2019/08/voter-privacy-act-would-limit-.html