Should government restrict online data collection to protect voters' privacy?

JEFFREY CHESTER
EXECUTIVE DIRECTOR, CENTER FOR DIGITAL DEMOCRACY

WRITTEN FOR *CQ RESEARCHER*, OCTOBER 2012

A political campaign sends a striking digital ad personalized to your age, gender, race, spending habits, location and favorite musician or TV show. That interactive ad later appears on your mobile device, gaming platform and computer screen as you surf the Web. Its message and visual content keep changing, as if it learned about you — including what you had most recently done online. Your best friend gets an ad from the same candidate, but with a different message. It seems you care about the economy, your friend about the Middle East.

Such scenarios are no longer fantasy. Campaigns, candidates and special-interest groups, tapping into the personalized data-mining capabilities of digital marketing, now can "shadow" or track voters wherever they go or whatever they do online — including using their mobile phones. Political groups can buy individual profiles that contain information culled from both online and offline data brokers, producing a "road map" to the specific issues likely to sway a particular voter.

Our digital dossier can include our race and ethnicity, gender, relationships, events that have affected us (a loan application or a medical treatment, for example), favorite websites and even our past actions (products purchased or videos viewed). It can access the torrent of social media information that tells not only about us but also about our relations with friends. New, interactive multimedia tools perfected for selling cars, computers and entertainment on websites and mobile phones make data-enabled voter ads even more effective.

We shouldn't allow voter decisions to be influenced by digital micro-targeting tactics that invade our privacy and set the stage for potential manipulation. As campaigns increasingly have the ability to tell each of us what they think we want to hear, the truth can easily become a victim. As tens of millions of finely tuned, personalized interactive ads are delivered to mobile phone screens, how will news organizations and other watchdogs effectively monitor the information to say what's right or misleading?

We are allowing powerful special interests — campaigns, candidates, super Pacs and the like — to build a vast data mining and targeting apparatus that is transforming our political process without public debate. Congress must step in to both protect the rights of voters and enact fair ground rules for digital political campaigns. Voters — not the K Street complex — should have the power to decide what online information can be collected and used.

JIM HARPER
DIRECTOR, INFORMATION POLICY STUDIES, CATO INSTITUTE

WRITTEN FOR *CQ RESEARCHER*, OCTOBER 2012

Just like marketers do year in and year out, political campaigns are doing everything they can at election time to learn the interests of voters and how to reach them. Is democracy better served by campaigns that know less about voters or by campaigns that know more?

Nobody loves the tawdry tone of electoral politics, and some of the obscure techniques campaigns use to gather voter information leave us squirming. But this is hardly a justification for laws that could blinder our political system.

Political privacy is an interesting beast. Some people are reticent to speak even with family members about their politics and their votes. Others put on garish costumes and post signs on their lawns and cars to advertise what they think. No law regulating how campaigns can collect and use information would hit the right notes for communities this diverse.

Instead of taking privacy off the table as a campaign issue, why not push it forward? This problem should be put to the politicians vying for votes. Their tact and skill in handling voter information is a signal of how they might handle things they oversee, such as government agencies' collection and use of citizen data.

It's not likely to be a top issue, but the use of data in campaigns might sway privacy-sensitive voters. A campaign data law would prevent this competition. Voters couldn't learn which candidates demonstrate sensitivity toward personal information. These are skills elected officials should have.

The best way to learn voters' preferences, just like consumers' preferences, is to hash things out through real-world experience. Rather than having lawmakers decide for all of us how data can be used in society, let voters and consumers render their judgments, casting their ballots and dollars with the candidate or marketer who satisfies them the most.

Privacy regulation is impossible to write well, easy to sidestep and, in the campaign area, contrary to free-speech principles, if not the actual First Amendment. The long-term solution for privacy problems has always been consumer empowerment and awareness, so that sensitive voters can hide their politics online as well as off.

Over time, people will learn how their electronic devices work to protect or expose them. Social practices will catch up with the rapid advance of personal information technology. And people will have political privacy to the extent they want it.