

# **California Secretary of State Kevin Shelley's Task Force on Voter Privacy**

**November 5, 2003  
Sacramento, California**

**Remarks by Kim Alexander, President & Founder  
California Voter Foundation  
[www.calvoter.org](http://www.calvoter.org)**

Good morning, thank you for inviting me.

The California Voter Foundation is a nonprofit, nonpartisan organization I established nearly a decade ago to advance new technologies to improve democracy. We are online at [www.calvoter.org](http://www.calvoter.org).

Over the years, CVF has worked with the California Secretary of State's office to harness the power of new technology to benefit the democratic process. California has pioneered the Internet's role in politics more than any other state, and has been at the forefront of a nationwide movement to bring campaign finances online and into the digital sunlight.

This task force is the first of its kind in the nation, perhaps even the world. It's an example of how California often finds itself on the cutting edge of democracy, and technology, and the places where democracy and technology intersect.

Technology brings new opportunities for electoral progress, but it brings risks as well. To better understand these risks as they relate to voter privacy, the California Voter Foundation has been studying voter registration data gathering and dissemination practices nationwide.

We decided to look into this issue because of growing concern about personal data privacy coupled with the increased practice of voter profiling -- that is, campaigns obtaining vast amounts of data about voters and using that data to precisely target specific voters for campaign messages. We wondered how much information is being collected from voters across the country, and what happens to it?

These questions are particularly timely now in light of last year's passage of the Help America Vote Act (HR 3295), which requires states to collect personal identifying numbers from registered voters and also requires all states to create and maintain standardized statewide voter databases. Under this new federal mandate, the amount of data collected from voters is increasing as well as being centralized and computerized. These changes make voter data more accessible than ever before.

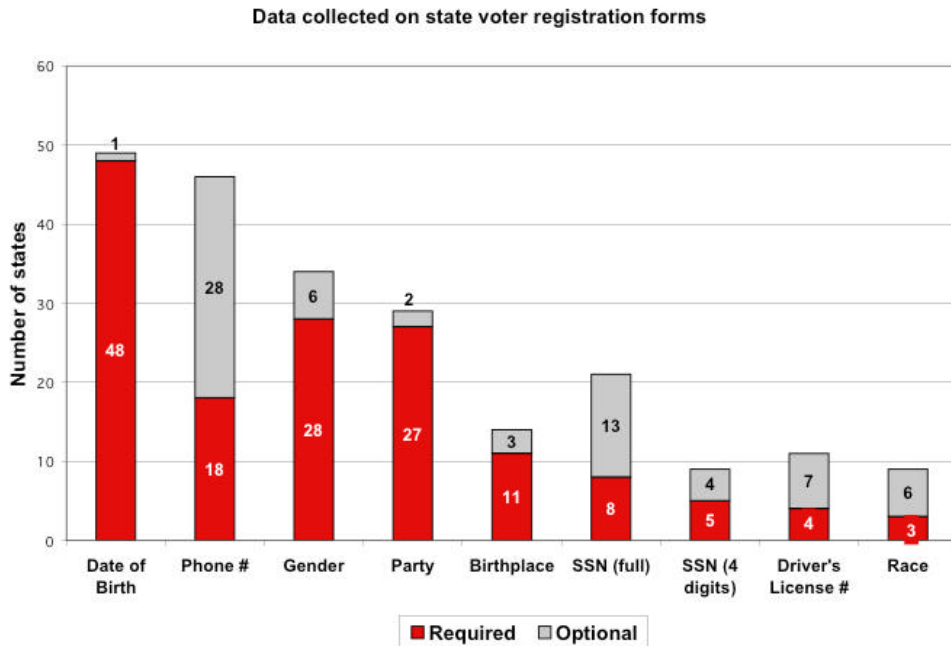
Last year CVF conducted a state by state study on voter data to answer five key questions:

1. What data is being gathered today on voter registration forms?
2. What notice is provided to voters on voter registration forms?
3. What data is added to voter registration records by election agencies?

4. What data is redacted or kept confidential?
5. What secondary uses of the data are permitted?

Today I'll give you a preview of our findings as well as recommendations, which will be published in a forthcoming study called "Voter Privacy in the Digital Age".

## Data Gathered



(Note: this summary of data gathered does not reflect changes made to forms in 2003 as required by HAVA -- all data is pre-HAVA)

- Name, Address, Signature. Every state form requires voters to provide their name, address and signature.
- Date of Birth. Every state requires voters to provide their date of birth, except Alaska, which makes it optional.
- Phone number. 46 states ask voters to provide a phone number. In 18 states a phone number is required; in 28 states it is optional. Four states require both a home phone number and a work/day phone number (AL, HI, KY, SC). Only three states do not ask voters for a phone number (NH, OK, VT).
- Gender. 34 states ask voters to declare their gender. 20 states require voters to state their gender in a "gender" field on the form, while eight states require voters to select a gender-specific salutation (Mr./Mrs./Miss/Ms.), which can also provide a female voter's

marital status. Five states ask for gender as an optional field on the form, while one state (CA) makes the salutation optional.

- Social Security number. 30 states require or request all or part of the voter's Social Security number (SSN) on their voter registration form. Of these, eight states require the full SSN (GA, HI, KY, MS, NM, SC, TN, VA) and 13 make it optional (AK, AL, AR, CO, DC, DE, IA, IN, LA, MD, NV, OH, TX). Five states require the last four digits of an SSN (FL, IL, KS, MO, OK) and four states make the last four digits optional (AZ, IN, UT, WV). (Changing under HAVA)
- Party affiliation. 27 states require voters to select a party affiliation (this includes Wyoming, which, even though it has no statewide form, does have a statewide requirement that the county forms collect party affiliation). Most state forms that require a voter to select a party also give voters the option to decline to state a party preference.
- Citizenship affirmation. 18 state forms feature a check-box requiring voters to affirm their U.S. citizenship (this is in addition to the general warnings and instructions that only U.S. citizens may register that are found on all forms). (Changing under HAVA)
- Place of Birth. 14 states ask voters to provide their place of birth, usually the city and state or foreign country. 11 states require voters to provide their place of birth (AL, AZ, CA, LA, NC, NH, NV, OH, TN, UT, VT); on three state forms providing a birthplace is optional (AK, MO, NE).
- Driver's License Number. 11 states ask voters for their driver's license number. Four states require voters to provide this number (IN, MI, NC, SD). Seven states make it optional (AR, CA, FL, NV, OK, TX, UT). Two states, Michigan and Indiana, use the driver's license number as a voter ID number. (Changing under HAVA)
- Race. 9 states ask voters to declare their race. 8 of these 9 states are southern states. 3 states require voters to provide their race (AL, NC, SC); in six states race is an optional field (FL, GA, LA, MS, PA, TN).
- Pollworker interest. 9 states ask voters to indicate whether they are interested in working at the polls on Election Day (AZ, AK, CA, CO, CT, IN, NJ, MO, VA).
- Special assistance at the polls. Four states ask voters to indicate if they need special assistance at the polls (AK, LA, FL, VA), and one state, Utah, has a "disabled" field as an optional field on its registration form.
- Parents' name. Three states require voters to provide a parent's name. Two states (LA and NE) require voters to provide their mother's maiden name and one state, Arizona, requires voters to provide either their mother's maiden name or their father's name.
- School district. Four states ask voters to declare their school district. Two states (NE, IA) require it, while two states (MI, MN) make this field optional.
- E-mail address. Two states ask voters to provide an e-mail address; both make this optional (CA and IN).

- Occupation. One state, Arizona, requires voters to provide their occupation.
- Indian Census number. One state, Arizona, has "Indian Census number" on its form as an optional field.

### **Notice to Voters: Five possible kinds:**

In order of prevalence:

1. Notice warning voters of penalties for providing false information on registration forms;
2. Notice informing voters of the reason for requesting Social Security numbers;
3. Notice telling voters which information fields are required to be completed, and which fields are optional;
4. Notice informing voters that their registration data is public record; and
5. Notice informing voters what secondary uses of the registration data are permitted.

#### **1. Penalty notice (100 percent)**

Every state form includes notice informing the registrant that by signing the form the registrant has avowed to the authenticity of their registration information. Many warn voters that they could be fined or serve jail time for providing false information or for registering to vote if they are not a U.S. citizen. Often such penalty notices are featured prominently on the form, in bold or capital letters. California's form now includes a new kind of penalty notice, warning that commercial use of voter data is a misdemeanor.

#### **2. Social Security number notice (two-thirds, 66 percent)**

While 30 states gather all or part of voters' Social Security numbers, only 19 state forms provide an explanation to voters for why this information is requested.

#### **3. Optional vs. Required notice (one-third/33 percent)**

38 state voter registration forms feature some fields that are designated as "optional;" 11 states do not feature any optional fields on their voter registration forms. For those states collecting optional information, some use the word "optional," while others use the words "requested," "if available" or "voluntary." One-third of the states collecting optional information were found to provide clear and consistent notice on voter registration forms as to which fields are optional.

California's voter registration form, which used to designate optional fields within the fields themselves, instead now designates optional fields in the instructions, sometimes with confusing language, such as: "No person shall be denied the right to register because of his or her failure to furnish a California driver's license or California identification card number. (Optional)." A similar notice for providing e-mail address is also included in the instructions. The two other optional fields on the California form, gender and phone number, have no similar notice accompanying their written instructions.

#### **4. Public records notice (4 percent)**

Of the 49 state voter registration forms evaluated, only four contain any notice to registering voters that the data they provide on the registration form is a matter of public record. New Mexico's form, for example, features a "Privacy Act Notice" in bold letters and the language, "Certificates of registration accepted for filing by a county clerk, and the contents therein, are public records open to inspection by the public." The other three states whose forms include such notice are Tennessee ("Voter registration records are public records, open to inspection by any citizen of Tennessee"), Texas ("Your voter registration application is open to the public"), and Iowa, which informs voters that their registration information may be disclosed to those who purchase lists of registered voters and "to those who view original voter registration records, which are public records under Iowa law."

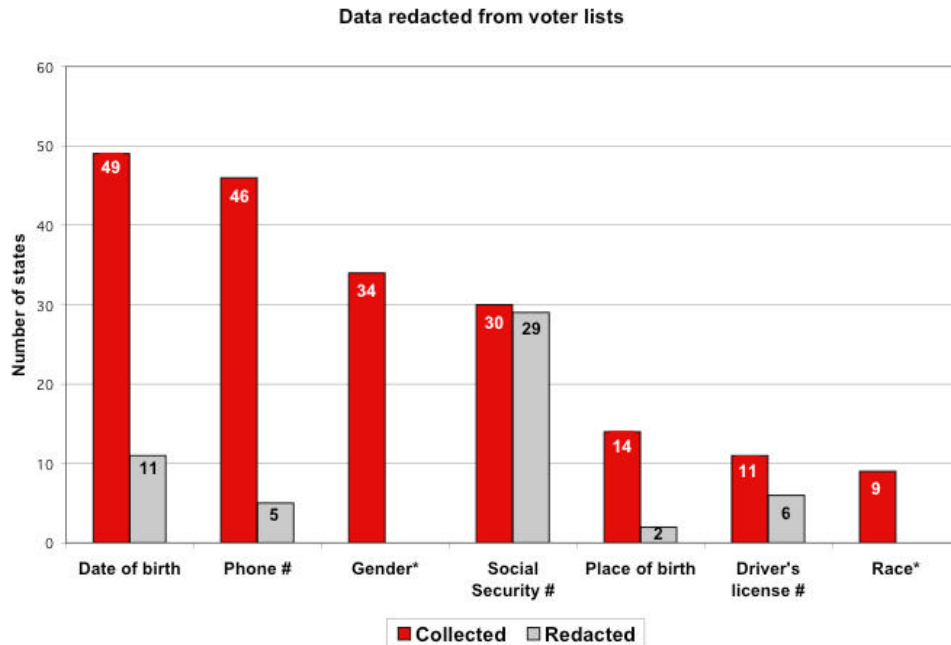
#### **5. Secondary users notice (2 percent)**

Only one state, Iowa, makes any specific reference to secondary users of voter registration data on their state form. New Mexico allows voters to choose whether they want their phone number to be "made public for election purposes." Last year California enacted a new law (AB 2832), that adds language to the top of the state's voter registration form stating that "the use of voter registration information for commercial purposes is a misdemeanor." However, the disclaimer is silent in regards to the secondary uses that are permitted under California law.

The overall lack of notice about secondary users, combined with inadequate notice about optional fields on the form, deprive voters of being able to make truly informed decisions about how much information they want to provide when registering to vote. In addition, voters are rarely informed at the time they register what purpose the optional information gathered will serve.

Prominent penalty notice on voter registration forms, combined with the lack of adequate public record, secondary uses, Social Security and optional notice, may be leading voters to part with more information than necessary when registering to vote, out of a desire to be "better safe than sorry." More robust notice would give voters the ability to exercise "informed consent" when registering to vote. Such notice, however, may also deter some people from wanting to register at all, which may be one reason why notice on registration forms is lacking in the first place.

## Redaction



- Of the 49 states collecting voters' date of birth, 11 redact some or all of the voter's birthdate from voter rolls. Seven redact voters' entire date of birth (AK, DC, HI, MS, NH, VT, WA). Four states redact a voter's month and day of birth (AZ, MI, MN, NM), enabling secondary users to deduce someone's age without knowing one's actual birthday. 38 states do not redact voters' date of birth from voter lists.
- Of the 46 states collecting voters' phone numbers, five states redact those numbers (GA, KS, MI, RI, WV), while 41 states do not.
- Of the 30 states collecting all or part of voters' Social Security numbers, all but one state, Iowa, redact this number from voter lists distributed to secondary users.
- Of the 14 states collecting voters' birthplace, only two states (AZ, VT) redact this information, while 12 states do not.
- Of the 11 states collecting driver's license numbers, six redact this number, including California (AR, CA, FL, IN, MI, NV, UT) and five do not (FL, NC, OK, SD, TX).

Voter record suppression. 27 states give certain voters the right to remove their individual record from voter lists obtained by secondary users (AZ, CA, CT, DE, FL, HI, IL, KS, LA, MA, ME, MN, MO, MT, NC, NE, NH, NJ, NV, OH, OR, RI, UT, VA, VT, WA, WI). The right to suppress one's voter record is generally given to those people who serve in sensitive public positions, such as police officers and judges, as well as those whose personal safety has been threatened, such as victims of domestic violence or stalking, and could

suffer harm if their contact information is published or distributed. Voter record suppression is not available in 24 states, including some of the most populous states, such as New York, Texas and Michigan.

### **Secondary Uses**

Administration of elections is the primary use for voter registration data. All states permit some secondary uses of voter registration data as well. Secondary uses fall into six categories:

- Political/election/campaign;
- Governmental;
- Commercial;
- Scholarly/academic;
- Media/journalistic; and
- Interest groups and nonprofit organizations.

### **Political uses**

Every state allows its voter registration data to be used for political purposes, which typically include sending campaign mail, precinct-walking and phone banking. Political campaigns and parties are the most common secondary users of voter registration data.

Because voter data is increasingly available in a computerized database format, it is not difficult for campaigns, parties or resellers to "add value" to this data or merge voter lists with other databases to enable campaigns to more precisely profile and target likely voters.

Computerized voter data is also easy for political parties to copy, enhance and redistribute on CD-ROM, via email and the Internet. Though the original recipients of the data most likely received it in a lawful manner, it appears that voter data is being routinely re-disseminated by political parties in violation of the terms by which they acquired the data in the first place.

The director of California's Democratic Party explained to a reporter last year how technology is speeding up campaign access to voter data: "People are constantly asking for target data. They'll want to know, how many Democrats with Latino surnames who voted in the primary and don't have a Republican in the household are in this precinct. In the old days you had to submit that to a computer person. Three or four days later they would get back to you. Now we can provide that information in a couple of hours." ( Dan Weintraub, "Pols will slice and dice to find niches in the electorate," *Sacramento Bee*, September 29, 2002.)

### *Voter profiling*

Because the burden of "educating" voters is placed on campaigns, it is therefore left up to campaigns to decide who gets informed and what they know. It is not in a campaign's interest to spend its time and money informing people who are not likely to vote for them, or at all. Consequently, the most likely voters are heavily courted by the campaigns while unlikely voters are largely ignored. While this has long been the case, the availability of

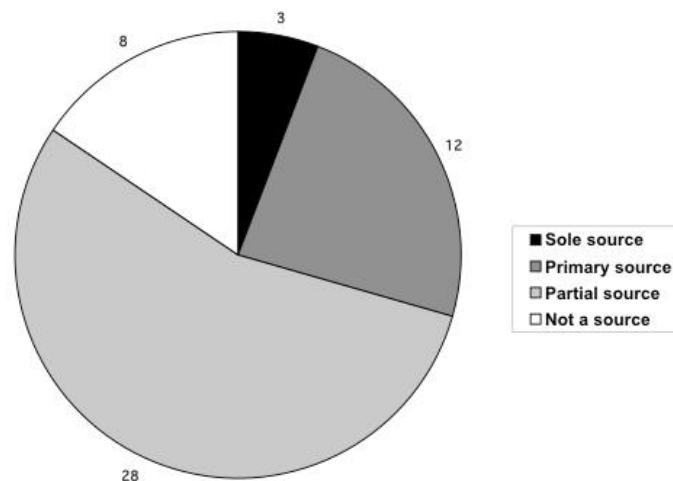
voter registration data in computerized formats has greatly enabled campaigns to even more precisely target their most likely supporters and ignore opponents and nonvoters altogether.

Demographically, nonvoters tend to be people who are younger, more transient, less wealthy and less educated than people who vote. If people who are not likely to vote are never courted by campaigns they are likely to remain nonvoters. Thus, voter profiling may be contributing to declining voter turnout.

## Governmental uses

### *Jury Duty*

States using voter lists for juror source lists



The most common and well-known secondary governmental use for voter registration data is for the selection of potential jurors; 43 states use voter lists as a juror source list. Three states rely solely on voter registration lists for juror lists (AR, MS, MT). In 12 states the voter lists are the primary source for juror lists while other government databases such as drivers' licenses data are secondary sources (CO, DE, GA, HI, ID, IN, MD, NV, ND, PA, SD, VA). In 28 states voter registration data is one of several sources used for juror lists. Only 8 states do not use voter registration data for juror lists (AK, FL, MA, ME, MI, NH, OK, WI).

Professor Stephen Knack has studied the likelihood of whether people are registered to vote based on their perception of juror source lists. In an analysis of data from the 1991 National Election Study, Knack found that:



- Of survey respondents who named voter registration lists as the sole source for juror lists, 71.4 percent were registered to vote;
- Of respondents who named voter lists and at least one other list as the source for juror lists, 77.1 percent were registered to vote;
- Of respondents who named drivers license or some list other than voter lists as a juror source, 82.1 percent were registered to vote.

These findings suggest that the more aware people are that voter lists are used for jury duty, the less likely they are to be registered to vote.

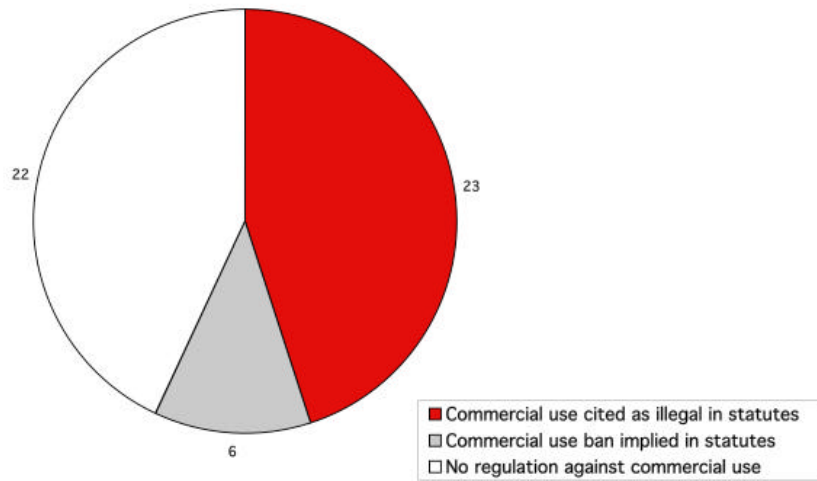
### *Incumbent mailings*

Elected officials access voter lists for their own campaigns; this widely permitted secondary use falls under the category of "political." However, these same politicians may, once in office, be able to use voter lists for mailings to constituents. In California, incumbent lawmakers sent out 7 million mailers to voters in the summer of 2002, all as official government business and at taxpayer expense. While California law forbids these mailers from being overt campaign advertisements, incumbents use them to boost their name recognition among targeted groups of voters. One Assembly member sent 47,090 women voters in his district a mailer about self-defense workshops. Another lawmaker sent a "Senior Legislative Update" to 35,000 elderly voters in his district. In one case, an Assembly member facing a tough re-election bid in a new Assembly district sent "constituent mail" to select voters who were not currently constituents, but were residents of the newly-drawn district. The total cost of the California Legislature's 2002 summer mailings was estimated to be \$3.5 million.

Such incumbent mailing practices raise several concerns. In addition to the imbalance this practice creates between incumbents and challengers, it is also apparent that lawmakers are now engaged not only in voter profiling but also constituent profiling. Legislators are elected to represent all people in their district, not only registered voters. While campaigns are free to choose whom they want to target, the idea of politicians using taxpayer dollars to inform select groups of voters is exclusionary and inappropriate.

### **Commercial use**

State statutes and secondary commercial use of voter lists



Twenty-two of the 51 states allow unrestricted access to voter lists (AK, AR, CO, CT, DC, DE, LA, MA, ME, MI, MS, NC, ND, NH, NV, NY, OH, OK, SC, UT, VT, WI). This unrestricted access permits the use of voter data for commercial purposes. None of these states' laws expressly identify commercial use of voter registration data as permissible; rather, these state statutes say that the data is available to anyone to use, or are silent about permitted secondary users altogether.

### Scholars and academics

Scholars and researchers use voter lists to conduct polls of voters and to analyze voter demographics and participation trends. That academics should have access to voter data is acknowledged in the statutes of only four states: California and Kentucky specifically permit "scholarly" uses of their voter data, New Mexico grants access for governmental research, and Iowa for "bona fide political research."

### The news media

Journalists use voter lists to determine whether candidates on the ballot have voted in previous elections; they also use voter lists for reasons unrelated to elections, such as finding an address or phone number when investigating a story. Only four states, California, Arizona, Kentucky and Indiana, expressly grant journalists access to voter lists in their laws.

The news media as an industry presents a dilemma when it comes to distinguishing permitted secondary users. On the one hand, news organizations are protected by the First Amendment and claim Freedom of Information Act rights to public records. On the

other hand, most news organizations are for-profit, and therefore are commercial enterprises; as such their access could be restricted in those states that prohibit commercial uses.

### **Recommendations for Protecting Voter Privacy in the Digital Age**

Through our research we have found that many states are gathering more data from voters than may be necessary for election administration, and that voter data is widely disseminated to secondary users, including commercial interests in 22 states, typically without any notice to voters that their information will be shared.

In considering policy recommendations to states for protecting voter privacy in the digital age, we acknowledge the need for elections agencies to collect sufficient information from voters for proper registration and administration. We also recognize that voter lists are a fundamental part of campaigns and elections. The following recommendations to states would achieve improvements in voter privacy while maintaining the integrity of election administration as well as the ability of campaigns to reach voters.

**1. Add notice language to voter registration forms stating that voter information is public record and explaining what secondary uses are permitted.** All states that collect Social Security numbers should comply with the Federal Privacy Act and notify voters of the reason for collecting this data. Citizens should have the right to be informed of the implications of disclosing their personal information as a condition of becoming an eligible voter.

**2. Place clear instructions and indicators on voter registration forms that explain which fields are optional and which ones are required.** The best way for a form to make this distinction is by putting the word "optional" both in the box for each optional field and in the instructions for those fields. For example, if an individual's telephone number is optional, the box for the field should read "Telephone number (optional)," with sufficient explanation in the instructions that explain why it is being requested so that the voter can make an informed choice about whether to provide it or not.

**3. Limit collection of data on voter registration forms.** For any field that is currently deemed "optional," state elections agencies should consider whether the particular information is absolutely necessary to administer elections. Information that is not necessary for election administration should be deleted from the form. State voter registration forms should follow as closely as possible the minimal-yet-sufficient standard of the universal application created by the National Voter Registration Act. In light of the federal "Help America Vote Act" requirement directing states to collect a "unique identifier" from voters in the form of their drivers' license number or the last four digits of their SSN, those states currently collecting voters' full SSN should reconsider doing so.

**4. Protect sensitive voter data.** Voters will be less worried about risks to their personal data if they can be assured sensitive data will not be redistributed to secondary users. The need to protect sensitive voter data will only grow in the coming years as states implement the new data-gathering requirements of the Help America Vote Act. Sensitive data, such as voters' birthplaces and exact dates of birth, should be redacted from voter lists as well. Seven states completely redact voters' date of birth, while four states redact voters' birth

day and month from voter lists, a step that enables secondary users to know a voter's age without knowing the exact date of birth.

Voters also need assurance that their election agencies are taking adequate steps to protect voter data from unauthorized access, negligence or hackers. Hackers routinely try to break into government computers and often succeed. For example, in May 2002 a hacker broke into the California state controller's computer system, which contains the personnel records for 260,000 public employees, including those in highly public positions, such as judges, politicians and university professors.

Internet-based registration-status or polling-place look-up services can be helpful to voters, but if not set up properly can also undermine voters' privacy. The Michigan-based Publius model, which uses the voter's address information to deliver correct polling place information online without actually displaying the voter's address or other personal data, is one that should be replicated.

**5. Prohibit commercial use of voter lists and voter registration data.** Already more than half the states prohibit commercial use of voter lists. Voting is a fundamental right that should not be exploited as a source of commercial solicitation. While the issue of whether news organizations and political data vendors should be classified as commercial users needs further debate, other nonpolitical commercial uses should be prohibited nationwide.

**6. Strengthen enforcement of laws that protect voter data from abuses by secondary users.** Policies restricting the duplication or commercial use of voter lists are rendered ineffective if elections agencies do not seriously attempt to monitor list usage and pursue cases of impropriety. Going after some high-profile violators would demonstrate a state's commitment to enforcing its laws regarding voter lists and may itself serve as a deterrent to improper use. More robust procedures for enforcing restrictions on voter registration data need to be developed and deployed.

**7. Consider applying the Federal Trade Commission's Fair Information Practices principles to voter registration data.** The standards that have come to codify the handling of personal information in Internet and other commercial transactions draw on a simple four-point plan known as the Fair Information Practices principles. The four principles are Notice, Choice, Access and Security, and provide a useful framework for a discussion about how to change and improve state voter data practices in ways that enhance voter privacy.

#### *Notice*

The Notice principle states that "consumers should be given clear and conspicuous notice of an entity's information practices before any personal information is collected from them." As described in Recommendation #1, voter registration forms should include notice language to voters.

#### *Choice*

The Choice principle "relates to giving consumers options as to how any personal information collected from them may be used for purposes beyond those necessary to complete a contemplated transaction." This principle enables a person to exercise a right

to approve or withhold the secondary usage of personal information. The Choice principle as applied to voter data could give voters the ability to choose which type of secondary users they wish to grant access to their data. The Choice principle could also enable voters to specify the way they prefer to be contacted by campaigns. For example, voters could indicate that they would like to receive mail from campaigns but not phone calls or door-to-door solicitations, thus establishing a kind of "Do Not Call" list.

### *Access*

The Access principle gives individuals the opportunity to have reasonable and appropriate access to information held about them, as well as a chance to amend or correct that information. For voters, it would mean being able to view their voter registration data, redact optional information if they choose, and change their preferences for whom they permit to use their data and how they want to be contacted. The application of the Access principle could also mean any voter, and not just those with special circumstances, could request their entire voter record be withheld from any secondary users. While this approach can limit the amount of data election agencies disseminate about voters in the future, it does not address data contained in voter lists that have already been disseminated and are in use.

### *Security*

The Security principle "refers to a data collector's obligation to protect personal information against unauthorized access, use, or disclosure, and against loss or destruction." As discussed in Recommendation #4, protecting the security of voter records requires the government agencies that house them to develop new security procedures that insulate the data from negligence, employee abuse and hackers.

## **Conclusion**

Voting is a sacred act of democratic life. We don't know the extent to which people's concerns about access to their personal data has kept some from voting. But we do know that a lot of sensitive data is being collected and shared and deserves better protection.

One reason the issue of voter privacy has received little attention in the past is because politicians who are in a position to regulate and protect voter data face a conflict of interest in doing so because they are also the biggest consumers of voter data.

As you consider the need to protect California voters' privacy, I urge you to keep the needs of all voters, and potential voters, first and foremost in your minds, and develop policies and decisions that first and foremost are in their best interests.

-----

### **California Profile:**

The voter registration form of the largest state features four optional fields, though the "optional" designation appears only in the instructions. E-mail is one of the optional fields, as California is one of two states seeking e-mail addresses from registrants. Driver's

license number is another optional field and, unlike all other information collected on the form, it is redacted from voter lists. Domestic-violence victims enrolled in a state program may have their voter records suppressed from voter lists. California has a statewide centralized voter database that may be purchased for \$30. Permitted uses are political, governmental, scholarly and journalistic. Commercial use is prohibited, with violations subject to a fine of \$0.50 per record.