Voter Privacy in the Digital Age

A Report by the California Voter Foundation

www.calvoter.org

Voter Privacy in the Digital Age

Findings from the California Voter Foundation's
2002 state-by-state survey of voter registration data
gathering and privacy practices

By Kim Alexander and Keith Mills
Published by the California Voter Foundation
www.calvoter.org

May 2004

For additional copies of this report, please contact:
California Voter Foundation
503 4th St. Ste B
Davis, CA 95616
(530) 750-7650

About this study

The California Voter Foundation (CVF) conducted a nationwide, state-by-state survey on voter registration data and the privacy implications of data-gathering and dissemination practices. CVF's goals with this project are to better inform public policy discussions about voter registration data and privacy, to educate the public about how voter registration data is currently being used, and to help develop policy solutions that address voter privacy in the digital age.

The California Voter Foundation and a team of graduate and law students from UC Berkeley researched the voter registration laws, forms, and data dissemination practices of all 50 states plus the District of Columbia. Research methods included: gathering and reviewing all state voter registration forms; researching state registration laws and regulations; and conducting interviews with election agency staff. The findings in this study are based on information collected during the Spring of 2002 and account for the registration forms, practices and laws as they existed at that time.

The California Voter Foundation is a nonprofit, nonpartisan organization advancing the responsible use of technology to improve the democratic process. More information about the California Voter Foundation is available online at www.calvoter.org.

Acknowledgements

"Voter Privacy in the Digital Age" is co-authored by Kim Alexander and Keith Mills, and was funded with a grant from the Wallace Alexander Gerbode Foundation. Research assistance was provided by Shalu Narula and Catherine Jesserand through the Samuelson Center for Law, Technology and Public Policy at the University of California, Berkeley. The authors are grateful to numerous colleagues and election administrators for their assistance in researching and developing this study. Please see the "Endnotes" section for a list of the people and resources consulted for this study.

Authors' Note

The California Voter Foundation and the authors of this study are deeply committed to improving voter participation. This study reveals many new findings about voter registration data gathering and dissemination practices that raise important questions and concerns about how to protect voter privacy in the digital age. It is not our goal to be alarmist or deter people from wanting to register to vote, but rather to be truthful with the public. Although raising awareness of voter data practices may in fact facilitate even greater access to voter data, it is our belief that the public's interest is best served in a democratic society by shining a light on an issue rather than by keeping the public in the dark. We hope this study facilitates a meaningful public discussion about the need to address new challenges to voter privacy in the digital age.

Table of Contents

Index of Charts

Key findings and recommendations

States are gathering a wide array of data from voters through voter registration forms:

- All states require voters to provide their name, address and signature;
- Every state but one requires voters to provide their date of birth;
- 46 states ask voters to provide their phone number;
- 34 states ask voters to declare their gender;
- 30 states ask voters to provide all or part of their Social Security number;
- 27 states require voters to select a party affiliation;
- 14 states ask voters to provide their place of birth;
- Eleven states ask voters for their drivers' license number;
- Nine states ask voters to declare their race;
- Four states ask voters if they need special assistance at the polls;
- Three states require voters to provide a parent's name;
- Two states ask voters to provide an email addresss;
- One state, Arizona, requires voters to state their occupation.

Of the five different kinds of notice to voters that appear on voter registration forms, penalty notice is the most common while secondary users notice is the least common:

- All state forms include a notice informing voters that by signing the form they are avowing to the authenticity of their registration information; many warn voters of potential fines or jail time for providing false information;
- 19 of the 30 states that collect Social Security numbers explain on the voter registration form the purpose for gathering this number;
- 13 of the 38 states that collect optional information from voters provide clear notice on their forms as to which fields are optional and which are required;
- Only four states indicate on voter registration forms that voter data is public record;
- Only one state, Iowa, makes a specific reference to secondary uses of voter registration data on its state registration form.

Some voter data is redacted before records are made available to secondary users:

- Eleven states redact some or all of voters' birthdates from voter rolls, while 38 do not;
- Five states redact voters' phone numbers, while 41 do not;
- All but one of the 30 states that collect Social Security numbers redact these numbers before redistribution to secondary users;
- Two states redact voters' birthplaces, while twelve do not;
- Six states that collect voters' drivers license numbers redact these numbers, while five do not;
- 27 states give certain voters the right to remove their records from voter lists obtained by secondary users.

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:

- All states grant candidates and political parties access to voter lists;
- 43 states use voter lists as a juror source list;
- 22 states allow unrestricted access to voter lists, which permits the lists to be used for commercial purposes;
- Four states grant scholars and academics access to voter lists under state statutes;
- Four states grant journalists access to voter lists under state statutes.

In considering policy recommendations to states for protecting voter privacy in the digital age, it is important to balance the need to protect voter privacy with the equally important need for election agencies to continue to collect sufficient information from voters to ensure proper registration and keep elections secure. It is also important to recognize that voter lists are a fundamental part of the campaign process. The following recommendations to states would improve 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 which secondary uses are permitted.

2. Place clear instructions and indicators on voter registration forms that explain which fields are optional and which are required.

3. Limit collection of data on voter registration forms.

4. Protect sensitive voter data.

5. Prohibit commercial use of voter lists and voter registration data.

6. Strengthen enforcement of laws that protect voter data from abuses by secondary users.

7. Consider applying the Federal Trade Commission's Fair Information Practices principles to voter registration data (Notice, Choice, Access and Security).

I.
Introduction

In the United States there are approximately 215 million eligible voters, and about two-thirds, or 144 million, are registered to vote.[1] One out of three eligible American voters remains unregistered to vote.

The chief purposes of voter registration are to prevent voter fraud and to facilitate election administration. An equally important but less well-known purpose is to provide political campaigns with contact and personal information about voters and their history of election participation. Campaigns have utilized voter lists for decades; a book dating from the 1920s examining the use of voter data shows that even back then campaigns were making use of voter registration lists.[2]

The role of voter data in political campaigns

The United States' electoral process relies on political candidates and parties to provide information to voters and promote voter participation. "Voter contact" is a key component to any successful political campaign, and campaigns use every means at their disposal to contact voters, especially those voters who are most likely to vote for them.

One way campaigns ensure that their message reaches the most desirable of voters is to know who those voters are in the first place. The key source of information about registered voters is the so-called "voter list," also called a "voter roll" or "voter file," that is maintained by election agencies. Voter lists are comprised largely of personal information supplied by voters when they filled out their voter registration forms. The most common types of information collected on voter registration forms include name, address, signature, date of birth, phone number, gender,

party affiliation, and all or part of the voter's Social Security number.

Voter lists as public record

Voter registration forms are processed by local election agencies, who input the data from the forms into voter lists. Voter lists are public record because they are government documents created by government agencies. If a state's laws do not explicitly permit the redistribution of voter lists, public records laws have been widely utilized as justification for redistribution to secondary users.

Public records laws serve to promote government accountability and protect the public against government secrecy. The notion that government records should be accessible to the public has a long tradition in the United States. Until digital technology made them more easily accessible, public records were characterized by "practical obscurity"— open, but often in limited formats and locations that reduce access to the records. Supreme Court Justice John Paul Stevens defended the notion of practical obscurity in a 1989 decision limiting journalists' access to criminal records compiled and computerized by government agencies. Stevens wrote: "There is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives and local police stations throughout the country and a computerized summary located in a single clearinghouse."[3]

The growing tension between public records and practical obscurity goes to the heart of voter privacy. On the one hand, a person's voter registration record is by tradition and law a public record because all citizens have an interest in ensuring the legitimacy of all voters and the integrity of the electoral system. On the other hand, widespread access to personal voter data can jeopardize a voter's privacy and safety.

Voter data exists in two distinct formats:

1. Actual registration forms held on file at an election office. These forms, also called "affidavits" are public records that meet the standard of practical obscurity, because anyone who wants to view the actual document must visit an election office and the forms can only be viewed one at a time. Some states block out certain information (such as a Social Security number or signature) from public inspections; many allow viewing but not copying.

2. Voter lists compiled by election agencies and consisting of the information supplied by voters on their registration forms. Before computerization, voter lists were protected to some degree by the notion of practical obscurity because such lists were available only on paper. Now that voter lists are widely available in a computerized format, they are also easy to duplicate, transfer and utilize in connection with other lists and databases. These computerized voter lists and the secondary uses of such data are the focus of this study.

The notion of personal privacy

The notion of a right to personal privacy is "nowhere but everywhere"[4] —it is not enshrined in the Bill of Rights or anywhere else in the U.S. Constitution[5], but most Americans have a reasonable expectation that they ought to be able to enjoy their space free of unwanted intrusion. A seminal work called "The Right to Privacy" established a concise definition that has come to dominate privacy discussions since its authors, Louis Brandeis and Samuel Warren, wrote it in 1890: "The right to be let alone." In 1967 Alan Westin updated the concept of information privacy with his influential book *Privacy and Freedom*. Westin defines privacy as: "The claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others." [6]

In the past two decades—a time roughly corresponding with the development of the computer age—public opinion polls have recorded a growing concern over the erosion of personal privacy at the hands of business and government. In 1978, a Harris poll on national attitudes found that 67 percent of Americans were concerned about threats to their personal privacy. By the mid-1990s, this same survey of American public opinion found that 84 percent were concerned about privacy, and polls in recent years continue to show a high level of public awareness of privacy threats.[7]

One important study on public records and privacy was conducted in 2001 by the American Society of Newspaper Editors and the First Amendment Center. In the survey, 50 percent of respondents said voter registration information "should not be made available to the public," while 47 percent said it should be made available.[8] These survey results show that when it comes to balancing the need for voter information with the need to protect personal privacy, the public appears to be divided.

The rise of identity theft, abetted by the unfettered exchange—and lax protection—of private personal information, has also raised awareness of how privacy breaches can harm consumers. The Federal Trade Commission reported in 2004 that identity theft persists as the top-rated complaint the agency has received over the past four years, comprising 42 percent of the nearly half million complaints logged by the agency.[9]

II.
Trends underway

To understand voter privacy in the digital age, one must consider the implications of current trends in technology, campaigning, and election administration. Computerization of voter registration data, the rise of voter profiling by political campaigns, and the implementation of statewide voter registration databases are important trends impacting voter privacy today.

Computerization of voter registration data

Voter lists, historically maintained and disseminated on paper, in recent years have been converted to a digital format, making election administration more efficient. Computerization also enables campaigns to acquire voter data in a digital format, making the data easy to copy, enhance and redistribute.

In the early years of computerization, there was little standardization of database formats, and the floppy disks and magnetic tapes that election agencies used to distribute digital voter lists limited transferability. Today, voter list databases are often distributed by state and local election agencies on CD-ROM and provided in standardized formats that can work in virtually any database program. Because the recipients of these databases, such as political parties and campaigns, receive the data in a user-friendly format, it is easy for them to redistribute voter data to others on CD-ROM, via e-mail and on the World Wide Web.

The director of California's Democratic Party explained to a reporter 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."[10]

The rise of voter profiling

Computerization has deeply impacted campaign strategy. Political campaigns have become much more skillful and precise in their efforts to target desirable voters. "Voter profiling" is commonly practiced by political campaigns as a way to maximize the campaign's financial resources and effectiveness.

Voter profiling has greatly enabled campaigns to precisely target their mail, phone calls and door-to-door visits to those people who are most likely to vote. In the process of precisely targeting whom they want to reach, campaigns have become skilled at ignoring those they are not interested in reaching—primarily nonvoters and infrequent voters.

In order to profile voters, campaigns first acquire a list of registered voters in their electoral jurisdiction, typically from their state or local election agency, their political party or a private vendor. In addition to providing personal and contact information, voter lists also include voters' history of election participation and often their preference to vote at a polling place or via absentee ballot.

Voter lists are often enhanced by campaigns, parties and private vendors who enrich the data by merging the lists with other databases that include more personal details about voters and their political preferences. Aristotle, the country's largest private vendor of voter data, maintains and sells records on 157 million American voters that contain each voter's registration data as well as their ethnicity, occupation, education, homeowner status and income level, whether they are catalog shoppers, and whether they have a history of making charitable or political donations. Aristotle's records also note how many voters live in each household and whether they are of the same or different political parties. Aristotle's records are accessible to virtually anyone in the world with a credit card and access to the Internet.[11]

The Internet is facilitating voter profiling in other ways as well. In 2000, online voter profiling helped get Sen. John McCain's presidential campaign on the Virginia primary ballot. In need of qualifying signatures, McCain had Aristotle match its voter profiles with the online profiles gathered from certain politically oriented Web sites. When a contracted site detected a Virginia Republican voter online, it displayed a banner ad inviting the voter to sign a McCain petition.[12]

Implementation of statewide voter registration databases

While voter lists have historically been maintained at the local level, in recent years a majority of states have started pooling the local records into one single statewide voter registration database. Currently, 37 states have a statewide voter database, updated at varying intervals. Several groups that issued election reform reports in the wake of the 2000 presidential election vote-counting

problems in Florida recommended that states implement statewide voter registration databases to ensure that registration data is streamlined and up-to-date in order to prevent the inadvertant disenfranchisement of eligible voters.[13]

The "Help America Vote Act" (HR 3295), enacted in October 2002, requires all states to create and maintain standardized statewide voter databases. While a single database will likely promote administrative efficiency, it will also provide secondary users with a single source of all voter records within a state. This lowers the time barrier and financial cost to secondary users for acquiring voter data. Instead of having to obtain voter lists from individual counties and towns, the buyer needs to interface with only one election agency in each state.

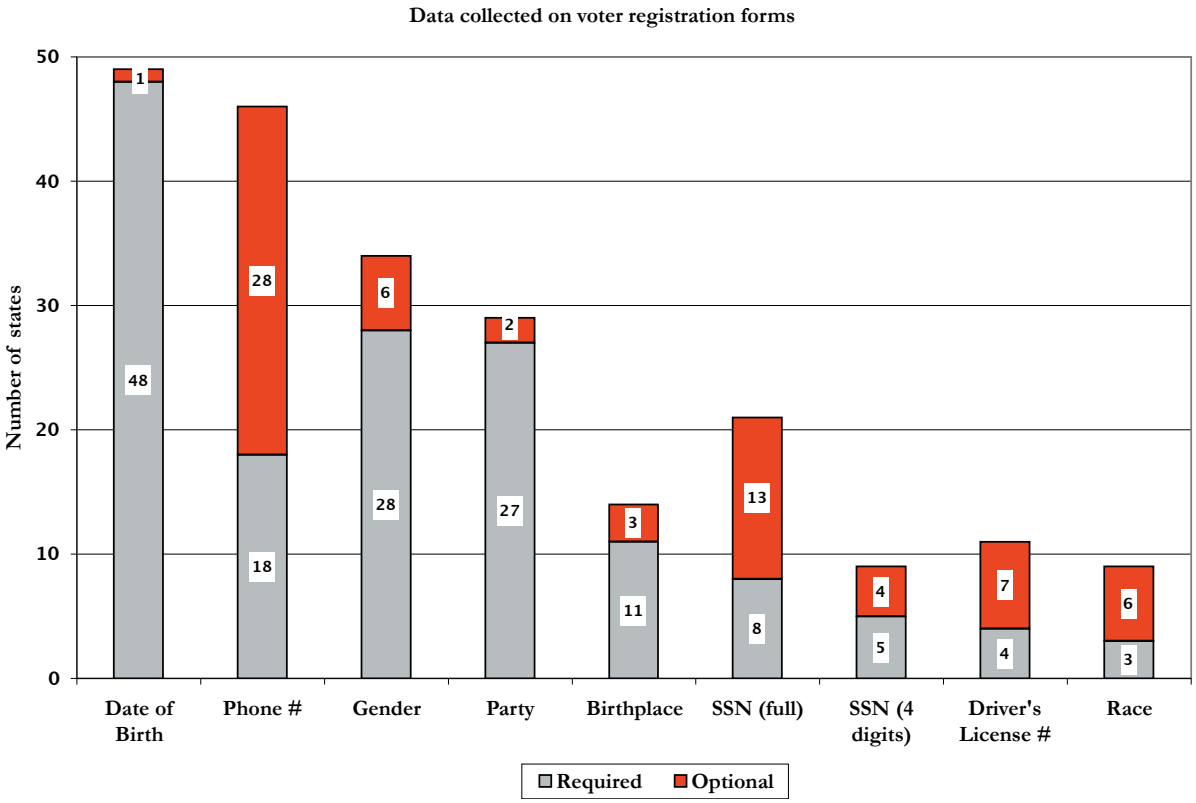
III.
FINDINGS

In conducting this study, seven essential questions relating to voter registration and privacy were considered:

- What data is being gathered today on voter registration forms?
- What notice is provided to voters on voter registration forms?
- What data is added to voter registration records by election agencies?
- What data is redacted or kept confidential?
- Which secondary uses of the data are permitted?
- How is information privacy regulated in other arenas?
- How is voter registration data being made available on the Internet?

A. Data gathered on voter registration forms

There is a wide variety of data gathered from voters on state voter registration forms. Below is a nationwide summary of data gathering, based on an evaluation of the 48 states that have statewide voter registration forms and the District of Columbia. (North Dakota has no registration requirement, and Wyoming conducts registration only at the county level.) A detailed chart showing what information each state gathers on its form is included in the appendix of this study.



• 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. Two states (LA, MD) ask voters to provide their age as well as their date of birth on voter registration forms.

• 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 provide 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).

• 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).

• Place of birth. 14 states ask voters to provide their place of birth, usually the city and state or foreign country. Eleven 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. Eleven 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.

• Race. Nine states ask voters to declare their race. Eight of these nine states are southern states. Three 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. Nine 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, 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, 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.

Federal data gathering requirements

• The National Voter Registration Act of 1993

The National Voter Registration Act of 1993 (NVRA) advises states to collect the "minimum amount of information necessary" when registering voters through motor-vehicle departments. The NVRA also directed the federal government to develop a "universal" voter registration form that "may require only such identifying information (including the signature of the applicant) and other information (including data relating to previous registration by the applicant) as is necessary to enable the appropriate State election official to assess the eligibility of the applicant and to administer voter registration and other parts of the election process."[14]

The NVRA form includes the following fields: name; address; gender (through salutation); date of birth; telephone number (optional); and three boxes that get filled in only if the applicant's state requires them: ID number (typically SSN or driver's license), party, and race. Fields not included in the NVRA form that appear on some state forms are: place of birth; parents' name; school district; e-mail address; occupation; pollworker interest; and the need for assistance at the polls. Voters using the NVRA form complete the application according to the directions for their state and mail it to their state's elections department. All but three states (NH, WI, WY) accept the NVRA form in lieu of their own.

• The Help America Vote Act of 2002

The Help America Vote Act (HAVA), passed by Congress and signed into law in October 2002, adds several new requirements that impact voter registration. While only eleven states are currently collecting driver's licenses, all of them will be required to do so in the near future, since HAVA requires states to collect voters' driver's license numbers when they register to vote. If a voter does not have a driver's license, HAVA requires the state to collect the last four digits of the voter's Social Security number. If neither number is available, HAVA directs states to assign the voter a number that will be used for voter registration purposes. States are also required to match the registrant's information with the state's drivers' database, and state motor-vehicle agencies are required to coordinate with the federal Social Security Administration to verify the accuracy of the registrant's information.

HAVA also requires states to establish centralized, computerized statewide voter registration databases to improve election administration. According to Electionline.org, 41 states have applied for waivers to delay implementation of this requirement until January 2006.[15]

B. Notice to voters

There are five possible kinds of notice, or disclosure to voters, that may be included on state voter registration forms. They are, 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.

Penalty notice

Every state form includes notice informing the registrant that by signing the form the registrant has avowed to the authenticity of his or her 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.

Social Security number notice

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. The Federal Privacy Act of 1974 requires "any Federal, State or local government agency which requests an individual to disclose his Social Security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it."[16] The eleven states that fail to provide such notice on their voter registration forms appear to be in violation of the Privacy Act. The breakdown is as follows:

States that provide notice:

Full number, required: six states (GA, HI, NM, SC, TN, VA)
Last four digits, required: three states (FL, KS, MO)
Full number, optional: ten states (AK, AL, AR, DC, DE, IA, ID, LA, MD, TX)
Last four digits, optional: 0

States that provide no notice:

Full number, required: two states (KY, MS)

Last four digits, required: two states (IL, OK)
Full number, optional: three states (CO, NV, OH)
Last four digits, optional: four states (AZ, IN, UT, WV)

"Optional vs. required" notice

When citizens register to vote, they are required to provide certain pieces of information on their voter registration form, such as their name and street address, while other pieces of information may be optional, such as their phone number. The "optional" voter information gathered through registration forms can be useful for election administration purposes; for example, it is much easier for an election agency to contact a voter about problems processing a voter registration form if the voter has provided a phone number.

38 state voter registration forms feature some fields that are designated as "optional;" only eleven 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." Of the 38 states that request optional information, only 13 provided clear and consistent notice to voters that the information requested was optional.

States use a variety of methods to inform voters on voter registration forms which fields are optional. Some state forms include the word "optional" in the field itself; some designate what is optional with an asterisk and a corresponding note at the bottom of the form. Some disclose which fields are optional through the written instructions featured on the form; these instructions may name the field itself (e.g. "Providing a phone number is optional"), or may reference a field number on the form (e.g. "Fields 5, 6 and 9 are optional"), thus requiring the voter to cross-check the field number with the field's content. Written instructions often appear at the bottom of the form, rather than the top, where voters would be more likely to review them before completing the form.

The New York, Georgia, Utah, California, West Virginia and Florida forms offer examples of inadequate optional notice. In West Virginia and Florida, the forms designate only those fields that are required or "must be completed," leaving it to registrants to deduce on their own that the remaining 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.

New York has two optional fields, home phone and gender. Both are indicated as optional in the instructions, but only one, phone number, is noted as "optional" in the field itself. Utah's form has a similar problem: phone number, last four digits of SSN, driver's license number and "disabled" are all optional fields; however, only the "disabled" field has the word "optional" appearing in the field itself.

Georgia's written instructions appear at the bottom of the form and list which fields are required. Three fields are optional on the Georgia form: race, gender and phone number. For these items, the instructions say, "Race and gender are requested and are needed to comply with the Voting Rights Act of 1965, but are optional. A telephone number where you can be reached during normal business hours is helpful to registration officials if they have a question about your application." While phone number is optional, it is not described by this term on the form itself, even though other optional fields are.

Texas sets a good example of a state voter registration form that clearly indicates what is optional. Texas places field-by-field written instructions at the top of its voter registration form. Optional fields are named and grouped together, enabling registrants to clearly understand which fields are optional. The instructions also notify voters that their record is public within the context of providing optional information. Texas' optional notice says: "Gender, Social Security Number, Telephone number and Driver's License Number or Identification Number are optional. The Social Security number is solicited by authority of sec. 13.122 and will be used to maintain the accuracy of the registration records. Your voter registration application is open to the public."

Twelve other states were also found to give voters good "optional" notice by including the word "optional" or "voluntary" inside the form fields and also providing information about optional fields in the form's instructions. These states include: DE, IA, IN, LA, MA, MD, MN, NM, NV, OH, PA, WI.

Public records notice

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."

Secondary users notice

Only one state, Iowa, makes any specific reference to secondary users of voter registration data on its state form. New Mexico allows voters to choose whether they want their phone number to be "made public for election purposes." California enacted a new law (AB 2832) that took effect in 2003, to add 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.

C. Data added to voter registration records

Election participation and preferred voting method

Every state keeps track of each voter's participation in each election; typically this data is added to voter lists and maintained by election departments. Many states also keep track of whether voters cast their ballots at the polling place or voted absentee. Many states that do not ask voters to declare their party affiliation on the registration form do track voters' party preferences when they vote in primary elections and incorporate this data into the voter list.

D. Data redaction

Data redacted from voter lists

State election policies redact some of the voter registration information before voter files are provided to secondary users. Below are a field-by-field summary and chart of data redaction practices.

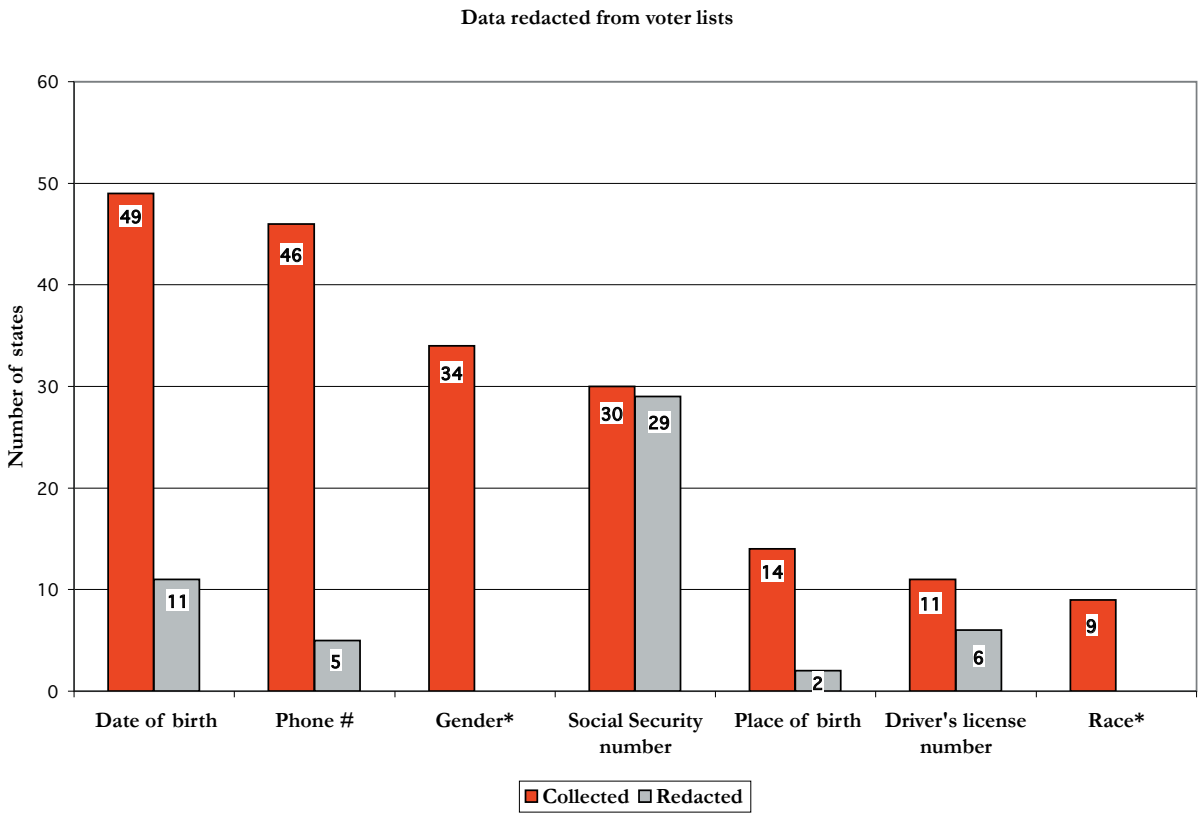
- Of the 49 states collecting voters' date of birth, seven redact voters' entire date of birth (AK, DC, HI, MS, NH, VT, WA). Four states redact a voter's month and day of birth (AZ, MI, MN, NM), enabling secondary users to deduce someone's age without knowing one's actual birthday. 38 states do not redact 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 twelve states do not.

- Of the eleven states collecting driver's license numbers, six redact this number (AR, CA, FL, IN, MI, NV, UT) and five do not (FL, NC, OK, SD, TX).



*No state that collects gender or race redacts this data from voter lists

Fields that appear on voter registration forms that are not redacted from voter lists at all include name, address, gender, party affiliation and race.

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.

The mechanics of how a state runs a voter record suppression program vary -- some offer total suppression, others remove only residential address and phone number from voter lists, and one (California's "Safe at Home" program) provides a mail-forwarding service so that a person's residential address is shielded by a common mailing address at the Secretary of State's office.

Only two states make reference to confidentiality programs on their voter registration forms. In Virginia, the voter registration form allows registrants who are active or retired law enforcement or who have a protective court order to declare their address as confidential. In Wisconsin, citizens enrolled in a state program for domestic violence victims may register to vote using a state-issued ID number instead of having to provide their name and address.

E. Secondary users

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

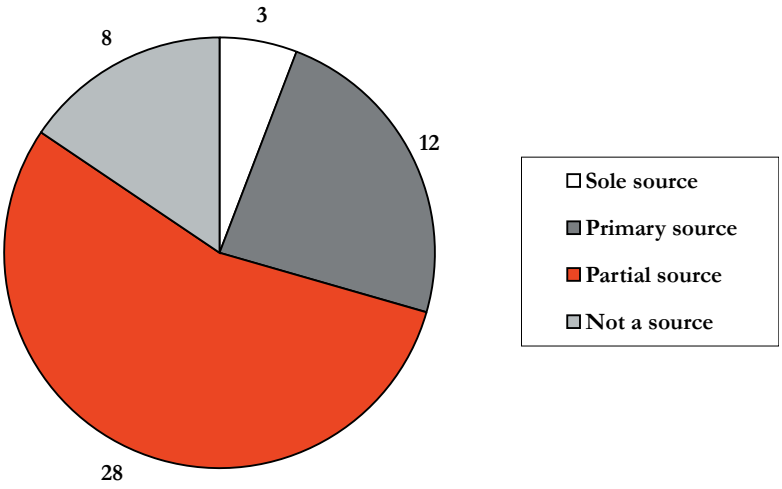
Every state allows its voter registration data to be used for political purposes, which typically include sending campaign mail, precinct-walking and phone banking. Political campaigns and parties are the most common secondary users of voter registration data. Campaigns typically obtain voter data by either purchasing it directly from their state or local elections offices, acquiring it from their political party, or buying it from political data vendors. Political data vendors profit from voter registration data and thus could be defined as commercial users; however they have been widely classified as political users because the campaigns to which they sell the data are using it for political purposes.

Because the 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. Voter profiling has become an integral component of modern campaign strategy, and is discussed in more detail in the previous "Trends underway" section of this study.

Governmental uses

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 twelve 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 eight states do not use voter registration data for juror lists (AK, FL, MA, ME, MI, NH, OK, WI).[17]

States using voter lists for juror source lists



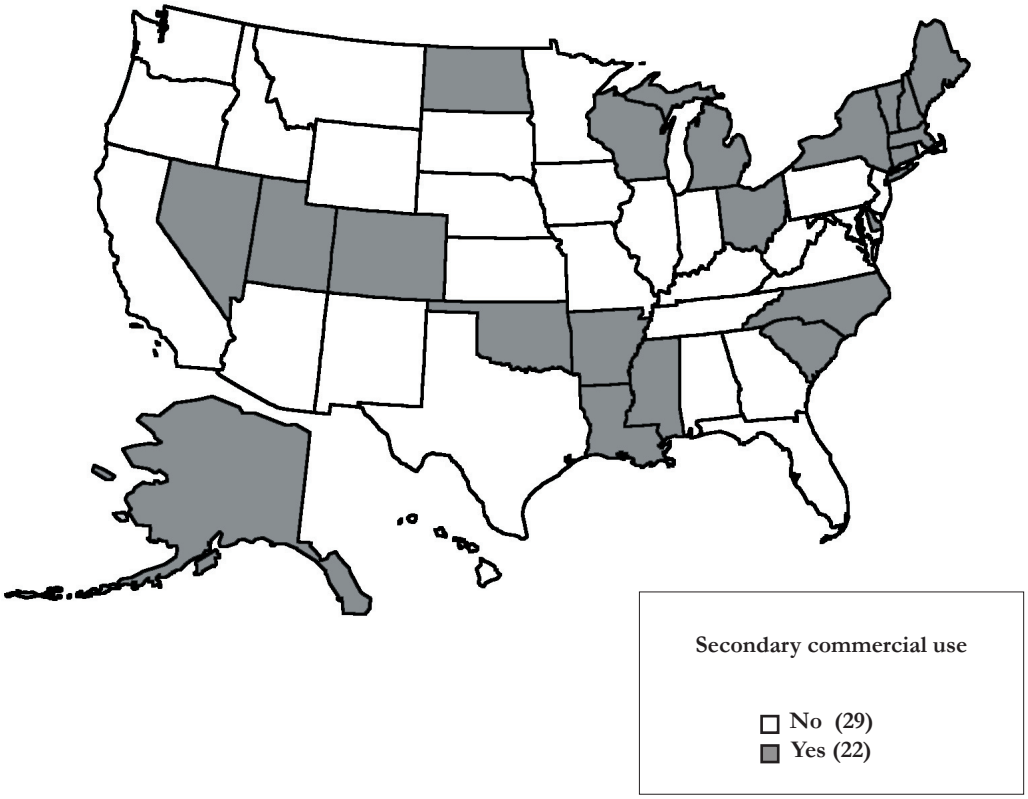
The government sector also uses voter registration data for the redistricting process. State legislatures are required to draw new districts every ten years to ensure that legislative districts within a state have a relatively equal numbers of residents. This legislative reapportionment is based on the federal Census, which provides information not only on the number of people residing in cities and neighborhoods, but also their race and ethnicity. State legislators also use voter lists as a political tool to guide the redistricting process, as the lists give information about the party affiliation of registered voters within a certain city, precinct or district. Using voter lists in this way, architects of redistricting can make a district "safe" for an incumbent or a particular political party or, alternately, make a district more attractive for a challenger.

Other governmental agencies, such as tax authorities and state employment agencies, may also use voter registration data to locate citizens. While only four states (FL, MN, NE, PA) explicitly state in their statutes that their voter records are open to law-enforcement inspection, law-enforcement agencies are typically classified as permitted governmental users of government records.

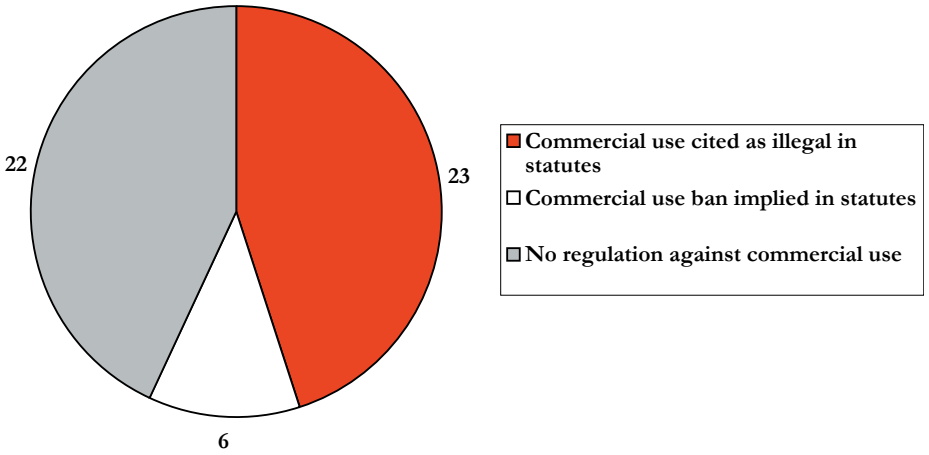
Commercial uses

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 unresticted 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. Of the 29 states that prohibit commercial use of voter lists, 23 expressly forbid commercial use (AZ, CA, FL, GA, HI, IA, ID, IL, IN, KS, KY, MD, MO, MT, NE, NJ, OR, PA, SD, TX, WA, WV, WY) and six states' statutes cite specific, permitted, non-commercial secondary uses and in this way restrict commercial access to voter lists (AL, MN, NM, RI, TN, VA).

Map: secondary use of voter lists



State statutes and secondary commercial use of voter lists



Other uses

Organizations other than those with political, governmental, or commercial interests may obtain and use voter lists for various purposes. These users include scholars and researchers, the news media, interest groups and non-profit organizations. Their access to voter information is uninhibited in those 22 states in which anyone may obtain voter lists. In the remaining states that specify permitted secondary uses, few have set a policy on usage for academic, journalistic or non-profit purposes.

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.

Interest groups and nonprofits

Political interest groups fall into a gray area of secondary users. While all the states allow access to political users, many do not consider political interest groups to be entitled to access voter lists. In states that distinguish between commercial and other types of usage, non-profit organizations, including interest groups, are generally held to be commercial unless there is an underlying election-related purpose. In the 22 states that permit any kind of secondary use, interest groups and nonprofits can acquire voter lists.

Interest groups that gain access to voter lists can combine them with other lists to more effectively target potential members. For example, the National Abortion and Reproductive Rights Action League (NARAL) reached beyond its Democratic Party base by targeting two million Republican and Independent women whose media preferences matched those of NARAL's existing membership.[18] In a similar vein, the Sierra Club used voter lists from

Pennsylvania and Ohio to identify 10,000 independent women voters and cross-referenced those names with other data sources indicating whether those voters would be responsive to solicitations from liberal organizations.[19]

Prices for voter lists

The cost of obtaining a voter list differs from state to state, and often from county to county within a state depending on the number of voters in a county. States have different ways of pricing their voter lists. Some states limit the fees charged to secondary users to the cost of materials and time, so that voter list buyers pay only for the cost of a CD-ROM and the time election agency employees put into fulfilling the request. Some states set a flat rate that each county may charge for its voter list. Other states price voter lists on a per-record basis; these rates range from a penny per name (Nevada) to $0.10 per name (Arizona). Prior to the passage of the Help America Vote Act, 37 states already had a statewide centralized database of all voters; many of these states charge a flat rate for a statewide voter list, with prices ranging from $30 (California) to $6,050 (Georgia). However, because these statewide lists are frequently not as current or detailed as local voter lists, many secondary users continue to rely on local election agencies to obtain voter data.

Penalties and enforcement

States with restrictions on secondary usage of voter lists attempt to prevent unauthorized usage in several ways. One method states use is to seed their voter lists with decoy names—a standard practice in the mailing-list industry—in order to identify subsequent users and abusers. In this way, if a purchaser of a voter list uses the list for some unauthorized purpose, the state will know about the abuse when it receives mail sent to the decoy name and address.

In the event of the discovery of an unauthorized use, states will apply penalties of varying severity. In California, misuse of voter lists results in a fine of $0.50 per name on the list; if the list purchaser acquires the entire statewide voter list of 15 million registered voters for political purposes but instead uses it for commercial purposes or redistributes it to someone else without prior written permission from the Secretary of State, the potential fine is $7.5 million. In Washington, which permits only political secondary users, an abuser of the data can be fined $5,000 and/or serve up to five years in jail.

F. Voter registration data and the Internet

There are three ways voter registration data can get put online: 1) if states put it online; 2) if counties put it online; or 3) if a secondary user, such as a data vendor, political party or public interest group, puts it online.

As of the November 2002 election, eleven states were offering online services that enabled residents of a state to look up their polling places, and in some cases, confirm their registration status (DE, GA, HI, IA, MA, MI, MN, NC, SC, VA, UT). An unknown number of counties also

were providing such services on their Web sites.

The most common system in use helps voters locate their polling places. After a voter submits his or her home address to the state election web site, the site displays the voter's polling place. Sometimes the site will also display a map showing the location of the polling place, as well as information about the races and measures that will appear on the voter's ballot. While this type of system requires voters to provide their home addresses, it does not display that address or any other personal information about the voter, thus preventing any voter data from being routinely disseminated over the Internet. Five states provide this type of service for voters (IA, MA, MI, MN, VA).

The state that pioneered this system was Michigan, where the Secretary of State partnered with Publius, a nonprofit voter education group, to provide voters with a registration and polling-place look-up service that does not display a voter's personal information. The Michigan system also allows a voter to log in using his or her name and year of birth. The site displays the voter's polling place and sample ballot for the next election, without displaying the voter's personal information.

Hawaii and Utah use similar online look-up services. Hawaii asks for the last six digits of a voter's Social Security number or information from the voter's registration confirmation postcard, while Utah requires a voter's name, county and date of birth. In both cases, the Web site displays only the polling-place address for that registered voter.

In addition to a simple polling-place address look-up, Virginia offers a secure access system that requires a state PIN number assigned by the state motor-vehicle agency to access voter registration data and status.

On Delaware's Web site, a voter can enter his or her name in order to confirm registration status, and the site displays the voter's name, city, zip code, polling place, and original registration date. While none of this information may be highly sensitive, the site does enable anyone to type in the name of a Delaware resident and find out if they are registered to vote.

In South Carolina, North Carolina, and Georgia, even more personal voter information may be accessed via the states' elections Web sites. South Carolina and Georgia ask voters to enter their name, county and date of birth. The site then displays the voter's name, full address, date of birth, race, gender, and polling place location, as well as a map showing the route between the voter's residence and polling place. Any Internet user who knows a South Carolina or Georgia voter's name, birthdate and county can access that voter's address online. North Carolina's look-up service asks only for a registered voter's name and then provides that person's city and zip code, race, gender, party affiliation, voter turnout history, and polling-place map. If the user provides a date of birth as well, the site will also display the voter's home address and voter ID number.

The potential consequences of using a date of birth as a password to access a voter's complete

information became evident when a nonprofit group, e-the People, experimented with online access to New York voter registration records in 2001. The New York site, Registeredtovoteo rnot.com, housed data for every registered voter in New York City. Visitors to the site could confirm their registration status and look up their polling place location by typing in their last name and birthday. The query returned the voter's full street address and party affiliation. Because there are many famous people who live in New York and are registered to vote, it was not difficult to find the birthdates of celebrities, type that date and their name into the site, and immediately find out where they live. The New York Times wrote a front-page story about the site;[20] shortly after it was published the site editors began redacting street address and party affiliation from the Internet display.

In addition to the growing number of states putting voter information online, political parties also utilize the Internet to disseminate voter lists to candidates of their party, often by giving candidates access to non-public, password-protected areas of their Web sites. While this practice generally does not conform with state laws that restrict redistribution of voter registration data, only two states, Arizona and South Dakota, have enacted statutes expressly prohibiting anyone from placing their voters' registration data on the Internet.

The easiest way to retrieve voter data online is to visit Aristotle's voter list service at www.voter listsonline.com. An Internet user needs only to provide a name, phone number, e-mail address and credit card to retrieve voter lists from every state except Arizona. Aristotle charges $25 per one thousand records. Aristotle also runs another site, Governmentrecords.com, where an Internet user can purchase a single voter's record for $25. Aristotle's services appear to violate the restrictions many states place on permitted secondary users of voter registration data. When selling data from states that restrict secondary usage, Voter Lists Online's order form refers to the appropriate state statute, preceded by a warning that "only qualified users can purchase data pursuant to applicable laws as stated below", and leaves it up to Internet users to determine whether or not they are permitted to access the data.

G. Information privacy regulation in other arenas

In the United States, the protection of personal privacy, including the handling of personal data, is based on a patchwork of government regulations and voluntary standards.[21] Private-sector transactions involving personal information have been largely unregulated by governments. Increasingly, however, commercial vendors who gain access to personal data, such as name, address and credit card information, are bound by self-imposed "privacy polices" dictating how they may use such data and what options a consumer has to control or limit use.

A 2002 study of Web site privacy policies found that nearly all of the most-visited 85 Web sites disclose their policies on handling personal information, and 93 percent offer the consumer a choice over sharing personal information with secondary users.[22] The Direct Marketing Association holds its members to a "Privacy Promise" that requires marketers selling customer lists to notify those customers of the practice and provide an opportunity to opt-out of the lists.[23] Consumers retain the right to limit their participation in such transactions in the

first place; they can choose to do business only with those who do not require or disclose information.

However, a person registering to vote does not have such choices. Privacilla, a Web site dedicated to privacy issues and edited by Jim Harper, puts it this way: "There is no question that protecting privacy in the commercial world can be hard. It is important to note, however, that protecting privacy from government is often impossible. When citizens apply for licenses or permits, fill out forms for regulators, or prepare tax returns, they do not have the power to control what information they share. They must submit information that the government requires. The first factor in privacy protection—power to control personal information—is totally absent in the governmental context."[24]

One prominent area in which recent federal legislation protects personal information whose collection is mandated by the government is driver records. The Driver's Protection Privacy Act (DPPA) of 1994 restricts access to state motor-vehicle records. Enacted in response to the murder of a young actress by a stalker who obtained her address through California driver records, the DPPA disallows public access to driver records as well as their sale for commercial purposes. Law-enforcement agencies, insurance companies, businesses performing ID verification, and investigators serving court business such as subpoenas are still allowed to access driver records under the DPPA.[25]

IV.
Discussion of findings

Implications of data gathered on state forms

Phone number

The fact that it is optional and not required for voters to provide a phone number in more than half of the states is an indication that this data is not essential for administration purposes. Only five states redact individuals' telephone numbers from voter lists; that most don't helps make voter lists very valuable to political campaigns and parties who rely on voters' phone numbers to conduct outreach activities. Political campaigns innovated the practice of telemarketing and for decades have relied on phone banks, often staffed by volunteers, to contact and influence voters. Today's political campaigns are taking telemarketing to a new level through the use of pre-recorded messages featuring the voices of politicians or actors. The campaigns use computers to auto-dial voters; if a voter is not home the pre-recorded campaign message is left on the voter's answering machine or voicemail system.

Sometimes the strategy is to make the pre-recorded call at a time when the voter is not home so that the message will be left on the voter's message system. As one company that sells such services advertised during the 2002 election, "Pre-recorded calls sent to live pick-ups are not only ignored, they are intrusive. A call delivered to an answering machine in your warm and sincere voice costs a very small fraction of a direct mail piece but has many times the vote-generating ability."[26] While this strategy may be effective for political campaigns, it also means that an increasing number of voters are receiving anonymous hang-ups if they answer their phones when such calls are placed.

Such practices may succeed in getting the campaign's message out, but at what cost? While it is unknown at this time whether political "voicemail spam" has a chilling impact on political participation, Congress did find, when it passed the Telephone Consumer Protection Act of 1991 (TCPA), that:

"[R]esidential telephone subscribers consider automated or prerecorded telephone calls, regardless of the content or the initiator of the message, to be a nuisance and an invasion of privacy."[27]

Although by law commercial enterprises are prohibited from placing pre-recorded calls, campaigns are allowed to do so because calls for noncommercial purposes are exempt under the TCPA.

Gender

Required in a majority of states, gender designations may provide election administrators with a useful breakdown of the voter population. But gender information also offers value to secondary users of voter lists. By matching gender and age information on voter lists, secondary users can know the demographic composition of a certain household's voters. In nine states the "gender" field consists of a salutation check box that includes the titles, "Mr.", "Mrs.", "Ms.", and "Miss". In selecting their salutation, female voters may also be providing their marital status, which can be a valuable demographic detail for secondary users.

Social Security number

The private, individualized nature of a Social Security number (SSN) can make it a reliable form of personal authentication. However, the value of an SSN in facilitating identity theft and other crimes has made the public more wary of disclosing their SSNs.

Voters who are concerned about identity theft will be relieved to know that Social Security numbers are redacted from voter lists in every state where they are collected, with the exception of Iowa. In addition, Aristotle, the largest broker of voter data, does not disseminate voters' SSNs.

While these redaction practices may give voters some comfort that their Social Security numbers are being protected, they do not address the fact that by merely collecting this data and storing it on government computers, election agencies put such sensitive data at risk of being accidentally or deliberately accessed by others. And while states today are redacting SSNs from voter lists, this has not always been the case; it has only been in recent years that the public and government have become more aware of the dangers of making SSNs widely accessible. It is likely that early purchasers of voter lists obtained and retain SSNs from states that collected them.

Though 19 states do provide some notice on their voter registration forms as to why SSNs are collected, another 11 states do not provide such notice; in seven of these states providing the

SSN is optional for voters, but without proper notice about why the number is requested in the first place, it is unreasonable to expect that prospective voters can make an informed decision about whether or not to provide their SSN.

In 1992, Virginia voter Marc Alan Greidinger sued his state over its requirement that he provide an SSN in order to register to vote. Specifically, Greidinger objected to a lack of notice on the form explaining why his SSN was being requested, as well as the fact that his SSN was available to view by any Virginia voter and disclosed on voter lists made available to secondary users. The court decision turned on whether the state's declared interest in preventing voter fraud outweighed the plaintiff's privacy interest. He won his case on appeal, with the court finding that "Greidinger's right to vote is substantially burdened by the public disclosure of his SSN."[28]

The appeals court directed Virginia to alleviate this burden by "either deleting the requirement that a registrant disclose his SSN or eliminating the use of SSNs in voter registration records open to public inspection and contained in voter registration lists." Prompted in part by the Greidinger suit, Virginia developed a Privacy Act notice to include on the top of the state's voter registration form. Today Virginia is one of only eight states requiring registrants to provide a full Social Security number, and it complies with the Federal Privacy Act of 1974 by informing voters that the purpose for collecting SSNs is to "ensure that no person is registered in more than one place," that their registration form will not be open to public inspection and that their SSN will "appear on reports produced only for official use by voter registration and election officials."

Place of birth, date of birth

Of the 14 states collecting voters' place of birth, only two (AZ, VT) redact this information from voter lists. Every state collects voters' date of birth, but only eleven partially or fully redact voters' birthdates from voter lists.

A person's birth date and birth place is private, personal information and so may function as a form of voter authentication. However, this information may be too personal to be appearing before secondary users. Knowing someone's place and date of birth, a would-be thief could obtain a birth record that can be used to commit identity theft.

Race

Only one of the nine states collecting race on their voter registration forms, Pennsylvania, is not located in the U.S. South. Six of these states are required to comply with the Voting Rights Act of 1965, which was enacted to redress historical patterns of racial discrimination in voter registration practices in the South. While race-based information is useful for these reasons of compliance, it has value for secondary users for different reasons: it enables voters to be sorted and targeted by race. None of the nine states collecting race information redact this data from voter lists. Three states that collect race information also allow secondary commercial use (LA, NC, SC). Even where race data is not collected on forms it is still utilized by campaigns. Data

vendors such as Aristotle gather race and ethnicity data from other sources, and campaigns often assume a voter's race or ethnicity based on surname.

E-mail address

Just as telephone numbers provide campaigns and marketers convenient access to voters, in the future e-mail addresses may become an even more important means of contact. This study found that only two states (CA, IN) are seeking e-mail addresses on their voter registration forms. But this is likely to become more common. A California elections official said that the state added e-mail as an optional field on its voter application because some counties were seeking an alternate way to contact voters. E-mail could facilitate communications between elections offices and voters; one could see a future in which election reminders and voter information guides are distributed to voters via e-mail. E-mail addresses are coveted by campaigns and marketers for different reasons. The cost of composition and delivery is lower than other means of communication, and the recipient can be targeted with customized content in the same way that campaigns currently target voters with direct mail.

Though few states collect voters' e-mail addresses, campaigns are able to gather e-mail addresses for voters from other sources to send out unsolicited campaign e-mail messages, also called "spam." Commercial restrictions on spam do not apply to political email because campaigns enjoy protected political speech under the First Amendment. Because campaigns rely on vendors to provide email addresses they often end up sending political spam to voters who are not eligible to vote for them. Such inefficiencies in political e-mail may give politicians greater incentive to seek changes to voter registration forms to include voters' e-mail addresses.

Driver's license number

A driver's license number is an existing unique identifier that can be used by election administrators for authentication and avoidance of duplication. Although in the past it was common for states to use one's Social Security number as the driver's license number, that is not the case anymore—every state issues a distinct number for its driver's licenses. Still, the driver's license number itself is of a personal, private nature and should not be made available to secondary users. However, five states do not redact voters' driver's license numbers from voter lists (FL, NC, OK, SD, TX).

The state of Michigan presents a unique case of using driver information to verify voter registration. In Michigan, the drivers' license number serves as a voter's registration number, and the state's computer files are linked so that changes to one's driver's license automatically update the voter's registration. This kind of verification system may become more common as states comply with the Help America Vote Act (HAVA), which relies on driver's licenses for voter verification.

Signature

A voter's signature cannot be data-entered into a voter list and therefore does not get redistributed through voter lists. However, this is changing. With increased use of early voting and mail-in balloting, some jurisdictions are beginning to convert voters' signatures into a digitized, electronic format to use when authenticating early voters or mailed-in ballots; in doing so, the signature becomes a government record and may be subject to public records laws. In Boulder County, Colorado, a voter-rights activist, Al Kolwicz, in 2002 purchased 75,944 digitized signatures on electronic tape from the county clerk's office for $50. According to the clerk, Charlotte Houston, "We did not like the idea of someone purchasing the tape that we keep signatures on. It was done because we could not find a legal option not to do it."[29] In response, the Colorado legislature enacted a law prohibiting the sale or disclosure of digitized signatures from voter files.[30]

Optional vs. required information

While most states gather "optional" information from voters, many state voter registration forms fail to include adequate notice clearly indicating which fields are optional and which are required, or what purpose the optional information provided will serve. While this lack of adequate notice may be due to poor form design, it also makes one wonder whether states are being intentionally vague in an attempt to collect more data from voters that will be useful to secondary users. Optional fields also raise the question of whether the optional data is truly needed to administer elections. Providing a phone number is optional in 28 states; if providing a phone number is not viewed as necessary for administering elections, then one must ask whether it really needs to be collected from voters in the first place.

Notice to voters

The overall lack of notice about secondary users, combined with inadequate notice about optional fields on the form, deprives voters of being able to make truly informed decisions about how much information they want to provide when registering to vote. 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.

Data added to voter registration records

All states add data to voter lists tracking each voter's turnout history in past elections. This information provides campaigns and other purchasers of voter lists with an idea of who is likely to participate in future elections. Campaigns can then target their message to reach those people who are most likely to vote and ignore those who vote infrequently or not at all.

Whether a voter has cast an absentee ballot or is registered as a permanent absentee voter is also often included in voter lists. This knowledge can be used to a campaign's advantage. If a campaign knows which voters will be receiving a ballot by mail before the election, it can target those voters early and not bother to call them on election day to "get out the vote."

Knowledge about who has requested absentee ballots can also play a role in facilitating absentee ballot fraud. In Texas, a voter's absentee status is made public, as well as the date when absentee ballots go out in the mail. These two pieces of information together enable campaigns to anticipate where and when absentee ballots are received by voters. In South Dallas, campaigns have long utilized "voter assistants" who show up on absentee voters' doorsteps the day their ballots arrive and "assist" those voters with casting their ballots. Texas also permits campaigns to return absentee ballots on voters' behalf. The combination of these laws and practices enables campaigns to engage in such "dirty tricks" as completing absentee ballots for residents in nursing homes and stealing ballots out of voters' mailboxes. National Public Radio reported that ballot "brokers" sometimes obtain stacks of absentee ballots, mark them, and then attempt to "sell" the marked ballots to political campaigns, threatening to destroy ballots favorable to a candidate if the candidate doesn't buy the ballots. [31]

Absentee voting is growing in popularity and many states are permitting greater use of absentee ballots as well as opportunities for voters to register as permanent absentee voters. As the South Dallas example shows, campaigns' knowledge of who the absentee voters are, combined with other election provisions, can lead to increased opportunities for voter fraud. If voter lists are to include absentee voting information, then states need to consider whether this information could facilitate voter fraud as has been the case in South Dallas. One Texas state legislator, Rep. Steven Wolens, has introduced a bill, HB 54 that would, among other things, require information about who has requested an absentee ballot to be made public the day after the election.

Voter record suppression and confidentiality programs

A growing number of states are attempting to address the need for voter privacy by creating special programs and procedures to protect the confidentiality of certain classes of voters, such as judges and victims of domestic violence. With 27 states already offering confidentiality programs to certain voters, the remaining 24 may consider doing likewise. Such programs demonstrate sensitivity that some people will refrain from voting if doing so requires them to make their personal information accessible and possibly place their safety at risk. However, these programs are only effective if they are publicized through channels that reach the classes of voters the programs seek to protect. A bigger policy question to consider is whether it's a good idea to continue singling out certain classes of voters for privacy protection, or whether any voter, for whatever reason, should have the right to keep their voter registration confidential.

Secondary users

Political uses: Voter profiling

All states permit campaigns to acquire voter lists; as discussed in the "Trends underway" section of this study, many campaigns "enrich" voter lists by adding data from other sources. Enriched voter lists enable campaigns to target voters by income, family size, homeowner status, occupation, organizational membership, magazine subscriptions, and political donations, thereby allowing campaigns to upgrade individual voter records into sophisticated voter profiles.

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 the perpetual decline in voter turnout.

Governmental uses: 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 Summer 2002 mailings was estimated to be $3.5 million. [32]

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.

Governmental uses: Jury duty

Since voter lists have been used for jury pools in many states for many years, the question of whether jury duty is a deterrent to voter registration has been considered by several scholars. It is a relevant question to consider in light of this study. If citizen awareness that voter data is used for a secondary purpose that may land them on a jury deters one's desire to register, then what impact will knowledge of other secondary uses have on registration and participation?

States can do one of three things with voter lists and jury duty: they can use only the voter lists to call jurors; they can use voter lists and other lists, such as licensed drivers lists, to call jurors; or they can use different lists altogether. 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.[33]

A study by Eric Oliver and Raymond E. Wolfinger found that individual knowledge of juror source lists has a small but detectable effect on voter registration status. Their study concluded that other factors, such as residential mobility and an interest in politics, are much more strongly correlated with registration status. They found that the perceived threat of jury duty may deter registration for a only small number of people, estimated at no more than two percent of the electorate.[34] Still, if as many as two percent of citizens are not registered in order to avoid jury duty, that represents potentially several million nonvoters.

Governmental uses: Law enforcement

Law enforcement may find new uses for voter lists in waging the War on Terrorism. Following the September 11, 2001 terrorist attacks, Congress passed the Aviation and Transportation Security Act, which mandates the creation of a "no-fly" list to be used to identify airline passengers that potentially pose a security risk. According to a 2002 San Francisco Chronicle article, the law requires the new Transportation Security Administration to coordinate with federal intelligence and law-enforcement agencies to share database information on individuals who may pose a risk to transportation or national security; already the CIA, FBI, INS and the State Department are contributing names to the "no-fly" list. The same article reported

that 20 Wisconsin anti-war activists were recently detained and questioned at San Francisco International airport, and that a Green Party activist was detained at a Maine airport last year.[35]

While it is not known whether voter lists are currently being used to profile airline passengers, factors such as one's party registration or voter turnout history might be useful for such purposes; those who vote frequently and are registered with one of the two major parties might be viewed as less of a risk than those who are registered with a minor party, or are not registered to vote at all. Voter lists may also be found to be useful to the U.S. government's new "Total Information Awareness" project, which seeks to bring together numerous public and private databases for the purpose of identifying people who pose a security risk.

Pricing

While the pricing method for voter lists varies from state to state, there is one characterization that fits across the board: voter information is an inexpensive commodity. This is due largely to the sense that voter lists are public records and therefore should be affordable.

The pricing for voter lists is, by the standards of commercial databases, quite low. In many cases, a statewide voter list consisting of hundreds of thousands or even millions of records can be purchased in electronic form for under $1,000. By comparison, proprietary commercial lists, such as a group membership or magazine readership, typically sell for $80 per one thousand records.

It may not be feasible for states to raise their list prices, however, because many states set such prices based on the fact that it is public data. As low as the prices are, state and local governments do make some money by selling voter data. Limiting secondary uses of voter lists will likely decrease a revenue source for state and local governments. This potential loss of revenue may lead some states and counties to resist attempts to limit the collection and dissemination of personal voter data that is valuable to secondary users.

Penalties and enforcement

Many states prohibit the resale or retransmission of a purchased voter list, yet parties, consultants and data brokers appear to be violating these laws as a standard practice.

The mechanism many states employ to catch unauthorized usage may be deficient. Seeding the voter list with distinct false names works as a tracking device if the user is merely copying the list and using it for mailings. But when the purchased voter list is merged into a larger database, the decoy names routinely are thrown out, because they do not match any existing records. Thus, the election agencies' key method for protecting data is routinely foiled.

In the early 1990s, a leading data vendor, Metromail, was accused of integrating and misusing voter data from states that prohibit commercial use. Metromail, which gathers and maintains information on individuals and sells it to businesses seeking to target their marketing efforts, had

added personal data from voter lists that it obtained from other secondary sources, including the AFL-CIO and Aristotle. Using such data was in direct violation of the laws of those states that prohibit commercial use of voter lists. Following investigations from Arizona and California, plus a front-page story in the Wall Street Journal, Metromail claimed that at first it had not known about the commercial prohibitions of some states but had later purged its databases of all voter data that came from those states. No state assessed a penalty.[36]

The Metromail case highlights the difficulty of enforcing laws against secondary use of voter lists. Making commercial use illegal means having to enforce the prohibition, which requires time, money and effort. Even then, actual evidence of misuse can be hard to track. It is difficult to determine whether a data vendor or other direct-marketing company that gains access to voter lists will in fact delete voter data from the records of those people living in the 29 states that prohibit commercial use.

Data security risks in government offices

One of the most important principles regarding information privacy is the need for data an individual provides to be held secure against improper access or disclosure. While privacy policies and regulations would represent a good step toward protecting voter privacy, they may not address another risk to voter data, that being accidental or intentional security breaches of government computers.

There are three basic ways that the security of government computers can be breached: 1) unauthorized access by government employees; 2) negligence; and 3) intrusion by hackers. There are many examples of such breaches in numerous government agencies that handle sensitive data on American citizens. For example:

• Unauthorized access: A study conducted by the General Accounting Office in 1997 revealed that hundreds of Internal Revenue Service employees had viewed the tax returns filed by friends, enemies, relatives and celebrities. In response, Congress enacted the Taxpayer Browsing Protection Act of 1997, which makes unauthorized browsing of federal taxpayer information a felony.

• Negligence: Government audits published in 2002 found that several federal government agencies cannot account for thousands of computers. The Customs Service lost track of approximately 2,000 computers while the Justice Department couldn't account for 400.[37] The Internal Revenue Service, which loaned 6,600 laptop and desktop computers to volunteers who provided tax-filing assistance to citizens cannot account for 93 percent of them. The IRS could also not guarantee that sensitive personal and financial information stored on those computers was removed as required.[38]

• Intrusion by hackers: Hackers routinely try to break into government computers and often succeed. 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. The personnel records include the kind of sensitive data, such as addresses and Social Security numbers, that can be used to financially or physically harm someone.[39]

V.
RECOMMENDATIONS

This study finds that many states are gathering more data from voters than may be necessary for elections 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. 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.[40] 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."[41] 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."[42] 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.[43] 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."[44] 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.

VI.
Conclusion

This study represents the first comprehensive analysis of voter privacy ever undertaken. One overarching conclusion of this study is the need to establish a national dialogue about how to protect voter privacy in the digital age and ensure that voter data practices are not a deterrent to voter participation.

It is not known the extent to which the voter profiling that arises from widespread access to voter data has already chilled voter registration and in turn, participation. Policymakers should consider this question and the steps that need to be taken for voter registration data practices to meet the needs of voters over those of secondary users. This will be a special challenge, since the politicians who ought to address this policy issue are also secondary users of voter lists and have come to feel entitled to widespread access to the data in order to run their political campaigns. Further, these politicians determine what data is gathered from voters and for what purposes it can be used. In many states the Secretary of State is responsible for maintaining the voter registration form and is also an elected officeholder. These roles may pose a conflict for an elected Secretary of State who may directly benefit from greater access to voter data.

Another challenge to implementing improvements in voter privacy is posed by the Help America Vote Act (HAVA). HAVA requires states to establish statewide voter registration databases, which can expedite the distribution of voter lists, and to collect and verify voters' driver's license numbers. The need to develop data management and privacy practices that protect voters has never been greater. Given that most states are redesigning their voter registration forms to comply with the new federal mandate, states have an opportunity to consider how their data collection and dissemination practices can be improved overall to better protect voter privacy.

Endnotes

1 Author interview with Curtis Gans, Committee for the Study of the American Electorate, September 2002.
2 Joseph P. Harris, Registration of Voters in the United States, Washington: The Brookings Institution, 1929.
3 Justice Dept. vs. Reporters Committee for Freedom of the Press, 489 US 749 (1989).
4 Brandon Garrett, The Right to Privacy, New York: The Rosen Publishing Group, 2001.
5 Ten states have explicit privacy rights in their Constitutions.
6 Alan F. Westin, Privacy and Freedom, New York: H. Wolff, 1967.
7 Ann Cavoukian and Don Tapscott, Who Knows: Safeguarding Your Privacy in a Networked World, New York: McGraw-Hill, 1997.
8 ASNE Freedom of Information Committee and the First Amendment Center, "Freedom of Information in the Digital Age," 2001, www.freedomforum.org.
9 Federal Trade Commission, "FTC Releases Top 10 Consumer Complaint Categories in 2003; Identity Theft Complaints Continue to Top List; Internet Related Fraud Complaints Soar", http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf.
10 Dan Weintraub, "Pols will slice and dice to find niches in the electorate," Sacramento Bee, September 29, 2002.
11 Aristotle International, Inc., www.voterlistsonline.com.
12 Leslie Wayne, "Voter Profiles Selling Briskly as Privacy Issues are Raised," New York Times, September 9, 2000.
13 See "Voting – What is, What Could Be", by the CalTech/MIT Voting Technology Project; "To Assure Pride and Confidence in the Electoral Process", by the National Commission on Federal Election Reform; and "Election Reform Briefing: Statewide Voter Registration Databases", by the Electionline.org and the Constitution Project.
14 42 U.S.C. 1973gg-5(a), (b), full text at www.usdoj.gov/crt/voting/42usc/subch_ih.htm#anchor_1973.
15 "Election Reform 2004: What's Changed, What Hasn't, and Why," Electionline.org.
16 The Privacy Act of 1974, 5 U.S.C. § 552A, www.usdoj.gov/foia/privstat.htm.
17 See "State Court Organization 1998" by the Justice Department's Bureau of Justice Statistics, www.ojp.usdoj.gov/bjs/abstract/sco98.htm.
18 Robert O'Harrow, Jr. and John Mintz, "Software Digs Deep Into Lives Of Voters; Campaigns' 'Profiling' Stirs Privacy Worries," The Washington Post, October 10, 2000.
19 John Mintz, "Political Groups Scramble To Find E-Mail Addresses," The Washington Post, October 22, 2000.
20 Amy Harmon, "As Public Records Go Online, Some Say They're Too Public," The New York Times, August 24, 2001.
21 Jacqueline Klosek, Data Privacy in the Information Age, Westport, Conn.:Quorum Books, 2000.
22 William F. Adkinson, Jr., with Jeffrey A. Eisenach and Thomas M. Lenard, "Privacy Online: A Report on the Information Practices and Policies of Commercial Web Sites," The Progress & Freedom Foundation, 2002, www.pff.org.
23 Direct Marketing Association, "Privacy Promise Member Compliance Guide," www.the-dma.org/library/privacy/privacypromise.shtml.
24 "Privacilla's Two-Part Definition of Privacy," www.privacilla.org/fundamentals/privacydefinition.html.
25 One way the private sector is getting around the DPPA is by gathering driver records directly from drivers when they provide their driver's license. In all but nine states a driver's data appears both on their license and is encoded in the license's magnetic strip. Many bars and night clubs have started utilizing scanners to verify patrons' age at the door; some also download and retain the patron's driver's license data gleaned from the magnetic strip, such as name, address, birthdate, height, weight and eye color, to be used for marketing purposes, and typically without the patron's knowledge. See "Bars, Stores Use High-Tech ID Scanners to Thwart Underage Sales," Foxnews.com, August 15, 2002, www.foxnews.com/story/0,2933,60464,00.html.
26 Ad for Win Your Race, Inc., on Campaignline.com.
27 47 USC 227, full text at www4.law.cornell.edu/uscode/47/227.html.
28 Greidinger v. Davis, 988 F2d 1344 (4th Cir. 1993), 1345-53.
29 Michael A. de Yoanna, "Voter signatures sold by county," Colorado Daily, April 26, 2002; accessed at www.users.qwest.net/~alkolwicz/news_042602_coloradodaily.htm
30 Colorado House Bill 02-1458, www.leg.state.co.us/2002a/inetcbill.nsf/fsbillcont/E4BDDE40E0E8B9F787256BA0007A8604?Open&file=1458_01.pdf.

31 Wade Goodwyn, "Absentee ballot fraud is tipping elections in Dallas," "All Things Considered," National Public Radio, July 25, 2002.
32 Greg Lucas, "Voters hit with mailers as budget sank: Incumbents last-minute blitz cost taxpayers millions," San Francisco Chronicle, September 15, 2002.
33 Stephen Knack, "Deterring voter registration through juror selection practices: Evidence from survey data," Public Choice 103: 49-62, 2000.
34 Eric Oliver and Raymond E. Wolfinger, "Jury Duty as a Deterrent to Voter Registration," Memorandum to the Board of Overseers of the National Election Studies," January 22, 1992.
35 Alan Gathright, "No fly blacklist snares political activists," San Francisco Chronicle, September 27, 2002.
36 Rick Wartzman, "Information Please: A Research Company Got Consumer Data from Voting Rolls," Wall Street Journal, December 23, 1994.
37 U.S. Department of the Treasury, Inspector General, "Protecting the Public: U.S. Customs Control Over Sensitive Property Needs To Be Improved (OIG-02-109), August 5, 2002.
38 U.S. Department of the Treasury, Inspector General for Tax Administration, "Computers Used to Provide Free Tax Help and That Contain Taxpayer Information Cannot Be Accounted For," Reference Number 2002-40-144, August 2002.
39 Sam Stanton and Ted Bell, "Hacking bares key data on all state employees," Sacramento Bee, May 25, 2002.
40 Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress," May 2000, www.ftc.gov/reports/privacy2000/privacy2000text.pdf. For more information about the FTC and other governmental agencies' fair information principles, see "A Review of the Fair Information Principles: The Foundation of Privacy Public Policy", published by the Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/fairinfo.htm.
41 Ibid.
42 Ibid.
43 Ibid.
44 Ibid.

VII.
Appendix

The following two charts show state-by-state voter registration data gathering and dissemination practices. This data was gathered in 2002 and reflects registration forms, statutes, and administrative practices at that time.

In the time since this data was gathered, Congress enacted the Help America Vote Act (HAVA), which includes provisions that require the gathering of additional voter data. It is likely that many state forms have been altered since 2002. These charts provide a valuable benchmark for understanding voter data gathering and dissemination practices in the pre-HAVA period.

The first chart, "State Voter Registration Forms, 2002", shows what specific fields of data are gathered by each state on its voter registration form. The second chart, "State Practices for Voter Registration Data, 2002", provides state-by-state details about practices ranging from the use of voter data for jury pools, record suppression, prices for voter lists, permitted secondary uses, and penalties for misuse.

State Voter Registration Forms Chart, 2002

State	Date of Birth	Social Security Number (Full)	Social Security Number (Last 4 Digits)	Work/day phone	Home phone	Gender	Party Affiliation	Race	Place of birth	Driver's License Number	Pollworker interest	Public Record Notice	Other Required Information	Other Optional Information
Alabama	•	on		•	•	•		•	•					
Alaska	o	on		o	o	•	•		o		o			Voter ID # ; special assistance?
Arizona	•		o		o*		•		•††				Parent; occupation	Indian Census #
Arkansas	•	on		o	o	•t	o			o				
California	•				o	ot	•		•††	o	o			E-mail
Colorado	•	o			o	•	•				o			
Connecticut	•				o	•	•				o			
Delaware	•	on			o									
District of Columbia	•	on		•		•t	•							
Florida	•		•n	o		o	•	o		o				Special assistance?
Georgia	•	•n			o	o		o						
Hawaii	•	•n		•	•	•								
Idaho	•	on			o	•t							Years of Idaho residency	
Illinois	•		•		o	•								
Indiana 1	•		o		•*	•				•	o			E-mail ("if available")
Iowa	•	on			•	•	•					yes	School district	
Kansas	•		•n		•*	•	•						Date residence established	"Naturalization data (if any)"
Kentucky	•	•		•	•	•	•							
Louisiana	•	on		o	o	•	•	o	•				Age; mother's maiden name; special assistance?	
Maine	•				•		•							
Maryland	•	on		•		•	•						Age	
Massachusetts	•				o	•t	•							
Michigan	•				o	•				•				School district (if known)
Minnesota	•				•									School district (if known)
Mississippi	•	•		•		•t		o						
Missouri	•		•n	o		•			o		o			

State Voter Registration Forms Chart, 2002, (continued)

State	Date of Birth	Social Security Number (Full)	Social Security Number (Last 4 Digits)	Work/day phone	Home phone	Gender	Party Affiliation	Race	Place of birth	Driver's License Number	Pollworker interest	Public Record Notice	Other Required Information	Other Optional Information
Montana	•				•									
Nebraska	•			o	o	•t	•		o				School district	Maiden name
Nevada 2	•	o			o		•		•	o				
New Hampshire	•						•		•					
New Jersey	•				o						o			
New Mexico	•	•n		o	o	•	•				o	yes		
New York	•				o	o	•				o			
North Carolina	•				•	•	•	•	•	•			Ethnicity (Hispanic or not)	
North Dakota 3														
Ohio	•	o			o				•					
Oklahoma	•		•				•			o				
Oregon	•				o		•							
Pennsylvania	•				o	•t	•	o						
Rhode Island	•				o		•							
South Carolina	•	•n		•	•	•		•						
South Dakota	•				•		•			•				
Tennessee	•	•n		•		•		o	•			yes		
Texas	•	on			o	o				o		yes		
Utah	•		o	o			•		•††	o				Disabled?
Vermont	•								•					
Virginia	•	•n		•		•					o			Special assistance?
Washington	•			•		•								Elect to be permanent absentee voter
West Virginia	•		o	o		o	o							
Wisconsin 4	•				o	•t								"ID Number" for those who suppress name/address
Wyoming 5							•							

State Voter Registration Forms Chart, 2002

State	Pre-qualifier	Penalty for false info
Alaska		misdemeanor
Alabama		jail term
Arkansas		jail term/fine
Arizona	U.S. citizen and not a felon	"class 6 felony"
California	U.S. citizen	perjury; jail term/fine
Colorado	U.S. citizen	"it is a crime"
Connecticut	U.S citizen	jail term/fine
District of Columbia		jail term/fine
Delaware		none cited: signature attests accuracy of info
Florida	U.S. citizen and not a felon	
Georgia	U.S. citizen	Felony
Hawaii	U.S. citizen, HI resident, 18 yrs old.	Class C felony: jail term/fine
Iowa		jail term/fine
Idaho	U.S. citizen and not a felon	perjury; jail term/fine
Illinois		perjury; jail term/fine
Indiana		perjury; jail term/fine
Kansas		jail term
Kentucky		jail term/fine
Louisiana		felony; jail term/fine
Massachusetts		perjury; jail term/fine
Maryland	U.S. citizen	perjury; jail term/fine
Maine		"Under penalty of law"
Michigan	U.S. citizen	perjury; jail term/fine
Minnesota		felony; jail term/fine
Missouri		perjury; jail term/fine
Mississipi		felony; jail term/fine
Montana		perjury; jail term/fine
North Carolina		"Class I felony"
North Dakota		
Nebraska		Class IV felony: jail term/fine
New Hampshire		perjury
New Jersey		jail term/fine
New Mexico		none cited: signature attests accuracy of info
Nevada		perjury/felony; fine
New York	U.S. citizen	jail term/fine
Ohio	U.S. citizen; "Do you want to register to vote?" •/no	"felony of the fifth degree"
Oklahoma		felony; jail term/fine
Oregon	U.S. citizen	jail term/fine
Pennsylvania	U.S. citizen	perjury; jail term/fine
Rhode Island		jail term/fine
South Carolina		Perjury

State Voter Registration Forms Chart, 2002, (continued)

State	Pre-qualifier	Penalty for false info
South Dakota		perjury; jail term/fine
Tennessee	Ever been convicted of a felony?	felony; jail term/fine
Texas	U.S. citizen	perjury; federal/state crime
Utah	U.S. citizen	"subject to penalty for false statements"
Virginia	U.S. citizen, not a felon, not mentally incapacitated	felony; jail term/fine
Vermont	U.S. citizen, take Voter's Oath	perjury; jail term/fine
Washington		Class C felony: jail term/fine
Wisconsin		perjury; jail term/fine
West Virginia		felony; jail term/fine
Wyoming		

Key: State Voter Registration Forms, 2002

•: Required field
o: Optional field
n: Notice given on form for collection of Social Security number.
t: Gender is collected as salutation (Mr./Mrs./Ms./Miss).
††: Place of birth is state/country, not city/state.
*: Phone number is required "if available" in IN and KS and is optional "if unlisted" in AZ.

1. Indiana requires the last 4 digits of an SSN if no other ID# is provided.
2. Nevada requires one ID number: SSN, driver's license, or other government ID.
3. North Dakota has no voter registration.
4. Wisconsin has voter registration only in cities and towns with more than 5000 residents.
5. Wyoming has no statewide voter registration form. Counties create their own forms to register voters.

State Practices for Voter Registration Data, 2002

State	Permitted secondary uses	VR as source of jury pool?	Info added to voter roll	Info suppressed	Record suppression possible	State-wide database	Prices for list or file	Regulation/ penalties for misuse
AK	All	no	Turnout history	SSN; date of birth	no	yes	$178 for statewide	Not defined
AL	political	partial	Turnout history	SSN	no	yes		
AR	All	sole source	Turnout history; party-primary voting*	SSN, driver's license #	no	yes	$250 for statewide; $50 for county disk	Not defined
AZ	political	partial	Turnout history	SSN; Month and day of birth; Parent; Place of birth; Indian Census #	Special classes of voters	yes	$.05 per name (paper); $.10 for CD, plus materials	Class 5 Felony for misuse (commercial use prohibited)
CA	political (current campaigns), governmental, educational, journalistic	partial	Turnout history; permanent absentee status	Driver's License #	Special classes of voters	yes	$35 for statewide; rest varies by county	$.50 per name penalty for commercial use
CO	All	primary	Turnout history	SSN	no	yes		Not defined
CT	All	partial	Turnout history; party*	SSN	Special classes of voters	yes: 145 of 169 towns	$300 for statewide	Not defined
DC	All	partial	Turnout history	SSN;date of birth	no	yes		Not defined
DE	All	primary	Turnout history; party	none	Special classes of voters	yes	$250 for statewide	Not defined
FL	governmental, political, law enforcement	no	Turnout history	SSN	Special classes of voters	yes		statute: penalty of perjury (sec. 98.0979)
GA	political	primary	Turnout history	SSN and phone number	no	yes	$6050 for statewide	statute: sec. 21-2-225
HI	political, governmental	primary	Turnout history	SSN; date of birth	yes	yes	$450 for statewide	misdemeanor
IA	political	partial	Turnout history	none	no	yes	~$2500 for statewide CD	"serious misdemeanor"

State Practices for Voter Registration Data, 2002, (continued)

State	Secondary uses	VR as source of jury pool?	Info added to voter roll	Info suppressed	Record suppression possible	State-wide database	Prices for list or file	Regulation/ penalties for misuse
ID	political	primary	Turnout history; absentee request	SSN	no	no	repro fees only	Sec 34-1815: $1000 fine and/ or 5-yr prison term
IL	political	partial	Turnout history	SSN	Special classes of voters	no	$2000 for state (all counties)	Class 4 felony
IN	political	primary	Turnout history	SSN		yes	$200 per county in file	
KS	political	partial	Turnout history	SSN; phone #	yes	yes		Commercial use is a Class C misdemeanor
KY	All	partial	Turnout history	SSN	no	yes		Not defined
LA	All	partial	Turnout history	SSN	Special classes of voters	yes	$50 per thousand (on CD)	Not defined
MA	All	no	Turnout history	none	Special classes of voters	yes		Not defined
MD	political	primary	Turnout history	SSN	no	yes		misdemeanor
ME	All	no	Turnout history	none	no	no		Not defined
MI	All	no	Turnout history; absentee status; voters per household	Month and day of birth; phone #; driver's license #	no	yes	$170 for statewide	Not defined
MN	political; law enforcement	partial	Turnout history	Month and day of birth	Special classes of voters	yes	$46 for statewide	misdemeanor
MO	political	partial	Turnout history	SSN	Special classes of voters	yes	$120 for statewide	Statute penalizes commercial use
MS	All	sole source	At discretion of counties	SSN; date of birth; phone #s	no	no	varies by county	Not defined
MT	"non-commercial"	sole source	no	none	Special classes of voters	yes	~$7750 for statewide	Bureau policy: No penalties stipulated
NC	All	partial	Turnout history	none	Special classes of voters	yes		Not defined

State Practices for Voter Registration Data, 2002, (continued)

State	Secondary uses	VR as source of jury pool?	Info added to voter roll	Info suppressed	Record suppression possible	State-wide database	Prices for list or file	Regulation/ penalties for misuse
ND	All	primary (from "actual voter" list)	Turnout history	n/a	no	no	varies by county	Not defined
NE	political	partial	Turnout history	none	no	yes		Class IV felony
NH	All	no		date of birth	Special classes of voters	no, but	~$1000 for statewide; $25 per precinct from local registrars	Not defined
NJ	political	partial	Turnout history; party	none	Special classes of voters	no	repro costs; not to exceed $375/ county	Commercial use: Fine of <$500
NM	political; governmental research	partial	Turnout history; voters per household (avail from counties only)	SSN and date of birth	no	yes	Varies by format: CPM of $1 to $15	Statute penalizes commercial use--$100 per record
NV	All	primary	Turnout history	SSN, DLN, Voter ID#	yes	no	$.01 per name	Not defined
NY	All	partial	Turnout history	none	no	no	repro fees only ($.25/ page)	Not defined
OH	All	partial	Turnout history; voters per household	SSN	yes- submit request in writing	yes	~$900 for statewide	Not defined
OK	All	no	Turnout history	SSN	no	yes	Statewide: $150. County: CD cost varies, $.25 per page	Not defined
OR	political	partial	Turnout history	none	no	no	varies by county	per Elections Division; civil penalty <$250
PA	election-related; law enforcement	primary	varies by county	none	no	no	repro fees only (per order of court case)	election-related functions only: 25 Pa. C.S. 1802

State Practices for Voter Registration Data, 2002, (continued)

State	Secondary uses	VR as source of jury pool?	Info added to voter roll	Info suppressed	Record suppression possible	State-wide database	Prices for list or file	Regulation/ penalties for misuse
RI	political	partial	Turnout history	phone #	no	yes		misdemeanor
SC	All	partial	Turnout history (avail on paper only)	SSN	no	yes	$1975 for statewide	Not defined
SD	political	primary	Turnout history	Description of residence location	no	yes	$2500 for statewide CD	Commercial use is a Class 2 misdemeanor
TN	political	partial	Turnout history	SSN	no	yes	materials cost	Class C misdemeanor
TX	political	partial	none (turnout history at county discretion)	SSN	no	yes		Class A misdemeanor
UT	All	partial	Turnout history	SSN, driver's license #	Yes, at county level	yes	$1000 for statewide	Not defined
VA	political	primary	Turnout history	SSN	Special classes of voters	yes		Class 5 Felony for misuse
VT	All	partial	Turnout history; party affiliation	Birthdate, birthplace	yes	No. Cities & towns only (not counties)	$.88 for a disk; $.04 per page	Not defined
WA	political	partial	Turnout history	date of birth	Special classes of voters	no		Felony: <5 yr. jail and/or $5000 fine
WI	All	no	Turnout history	none	Special classes of voters	no	repro fees only	Not defined
WV	political	partial	Turnout history	SSN, phone #	no	yes	$.015 per name	misdemeanor
WY	political	partial	none	SSN	no	yes		misdemeanor: < 6 mo. jail and/ or $1,000 fine