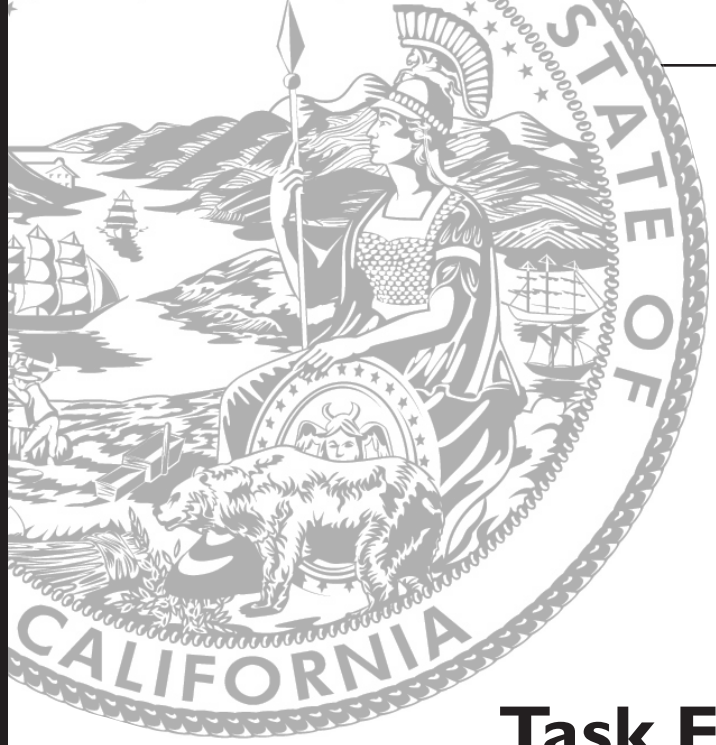

Task Force on Voter Privacy
FINAL REPORT

Chair
Willie L. Pelote, Sr.

Members
Linda Berger
Bill Cavala
Beth Givens
Jim Hayes
Victor Salazar
Dave Wong

presented to **Secretary of State Kevin Shelley**
and **Members of the Legislature**

June 14, 2004

Task Force on Voter Privacy

June 14, 2004

The Honorable Kevin Shelley
Secretary of State
1500 - 11th Street
Sacramento, CA 95814

Dear Secretary Shelley,

Attached for your consideration is the final report of the Task Force on Voter Privacy which was constituted under authority granted by Election Code Section 2195 (AB 2832, Chapter 959, Statutes of 2002).

On behalf of the members of the Task Force allow me to thank you for the opportunity to serve the voters of California in this important endeavor. The need to protect voter information from fraud, abuse and commercialization is critical as the threat of identity theft and other crimes remains a challenge in California and across the nation. Û

Contained in the Task Force's report are various policy recommendations which we developed in response to substantial and compelling testimony received at the four public hearings convened throughout the state last year. We appreciate your interest in ensuring the privacy of voter information and look forward to working with you, the Legislature and the Governor to codify these recommendations.

Sincerely, Û

Willie L. Pelote, Sr. Û
Chair, Task Force on Voter Privacy Û

Task Force on Voter Privacy
Final Report

Table of Contents

Introduction

Assembly Bill 2832 (Shelley, Chap. 959, Stats. of 2002) mandates that a seven-member Task Force[1] be appointed by the Secretary of State to study and recommend standards for protecting voters' private information that is contained in the voter registration file (Elections Code Section 2195).[2] With the enactment of this legislation, the legislature intended to ensure the protection of private information contained in voter files without stifling access to information necessary to facilitate and encourage participation in the political process.

The voter registration file is the repository for information supplied by citizens when they register to vote. Current law requires that voter information be kept confidential, except for political or governmental purposes. In order to gain access to voter information, an application must be submitted to a county elections officer or the Secretary of State. Under current law, elections officials, journalists, scholars can use voter registration information, campaigns, candidates, political parties and their central committees for certain prescribed uses. Commercial use of voter file registration information is prohibited.

Under current law, additional privacy protection is afforded to certain classes of people including domestic violence and stalking victims and reproductive health care workers when they provide specified documentation that supports the need for confidentiality (Elections Code Section 2166.5). These persons are entitled to strict confidentiality under which no person is entitled to access their personal information contained in the voter file. Current law also provides this same protection for any person, upon order by a Superior Court Judge, when there is a finding that the person, or a person in their household, faces life-threatening circumstances (Elections Code Section 2166).

With this information in mind, the Task Force held four public hearings to discuss the following topics: Overview of Voter Privacy Issues; Keeping Forms and Documents Private; Confidentiality Issues and Enforcement of Current Laws; and, The Voter File-Access and Privacy. The ultimate intent of the Task Force is to make recommendations to strengthen public confidence on privacy issues, and to ensure that voters receive, and are contacted about, information that is pertinent to them.

The Task Force is comprised of the following individuals:

Willie Pelote, Political Director, AFSCME (Chair)
Linda Berger, Executive Director, Statewide California Coalition for Battered Women
Bill Cavala, Speaker's Office of Member Services
Beth Givens, Director, Privacy Rights Clearinghouse
Jim Hayes, President, Political Data, Inc.
Victor Salazar, Fresno County Registrar of Voters
Dave Wong, President, San Francisco Deputy Sheriff's Association

[1] See Appendix A for additional information on Task Force Members
[2] See Appendix B for Elections Code Sections pertaining to voter file information confidentiality

Executive Summary

Over the course of four public hearings, the Task Force on Voter Privacy heard from numerous witnesses regarding the use of voter registration information permitted under current law by:

- Journalists, serving as the public's "watchdog," who may use voter file information, in part, as the source of stories that address the integrity of the election and redistricting processes;
- Scholars, who may use voter information data for studies on voting patterns, voter turnout and for survey purposes;
- Campaigns, candidates and political parties, who may use voter file information to provide voters with information about issues and candidates, and encourage voter participation, including voting on Election Day or by absentee ballot; and,
- Governmental agencies, which may use the voter file for purposes ranging from law enforcement personnel seeking to establish a person's identity to jury commissioners who use the voter registration file along with data collected by the Department of Motor Vehicles as a source to randomly select potential jurors.

The dates and topics of the Task Force's four public hearings were:

- November 5, 2003 – Overview of Voter Privacy Issues
  The Task Force heard testimony regarding current efforts in California to keep voter file information private and where these efforts fall short.
- November 12, 2003 – Keeping Forms and Documents Private
  This hearing included testimony regarding the collection of voter information and the potential misuses of this data. The Task Force heard testimony about issues related to voter information provided on forms (such as initiative petitions, voter registration cards, provisional ballots, etc.) Topics included types of access that should be provided for this information, how this information is handled, and what kind of notice is provided to voters.
- November 21, 2003 – Confidentiality Issues and Enforcement of Current Laws
  The Task Force heard testimony about confidential voter registration status. Topics included whether elections officials should keep certain people off of the voter file, the enforcement of current laws protecting voter data, and the enforcement of related laws.
- December 15, 2003 – The Voter File – Access and Privacy
  The Task Force heard testimony from county elections officials describing current procedures assuring voter privacy – and the steps taken when county elections officials require additional guidance. Topics included whether access by vendors to the file and current law prohibiting nonpolitical commercial access to this information are adequate and how sensitive voter data are controlled and protected.

The Task Force was presented testimony emblematic of an overriding public interest in maintaining confidentiality for certain persons. For example, domestic violence and stalking victims who face potentially life-threatening circumstances at the hands of abusers who will go to almost any lengths to discover the whereabouts of those they victimize.

The Task Force was presented testimony on the fastest growing crime in the nation, victimizing millions of Americans every year—identity theft. Personal information contained in the voter file, while by itself may not be enough to allow a crime to be perpetrated, can be combined with other personal information making a person more vulnerable to identity theft. The Task Force also considered how newly enacted federal law concerning the collection of driver's license numbers and partial Social Security numbers may affect voter privacy concerns.

Finally, the Task Force heard from numerous parties about the practical application and enforcement of state law. The Task Force also pursued independent research to reach its policy recommendations.

Throughout the proceedings, the Task Force members and witnesses spoke publicly about the difficult task of balancing sometimes-conflicting goals:

- The openness and accountability required of every legitimate democracy and the constitutional provisions for anonymity, including the secret ballot and constitutional protections of individual privacy;
- The need to inform voters of the use of voter file information by someone other than elections officials, and the impact such notification can have on suppressing voter participation;
- The statutory entitlement and public-policy goals served by allowing access to the voter file and the difficulty of enforcing restrictions that limit its use to the four exceptions: scholarly, journalistic, political or governmental purposes.

With the following ten recommendations, the Task Force is seeking to strengthen public confidence in the electoral process by achieving an equitable balance in a progressively sophisticated technological age:

1. **Notify voters about secondary uses of voter registration information;**
2. **Identify more clearly optional information on voter registration form;**
3. **Clarify voter registration requirements;**
4. **Sponsor legislation to limit uses of voter registration information;**
5. **Sponsor legislation to clarify voter privacy best practices and uniformity;**
6. **Propose legislation to increase criminal and civil penalties for misuse of voter information;**
7. **Ensure secure design of statewide voter registration database;**
8. **Safeguard against voter intimidation in the ballot measure, referenda and recall processes;**
9. **Require additional safeguards by vendors authorized to use voter registration information;**
10. **Prominently display criminal penalties for theft or removal of voter rosters at polling places.**

Public Hearings

HEARING #1 - November 5, 2003—Sacramento, California

OVERVIEW OF VOTER PRIVACY ISSUES

Testimony at this public hearing was provided by:
Kim Alexander, President and Founder, of the non-profit California Voter Foundation
John Mott-Smith, Chief of the Elections Division for the Secretary of State.

SUMMARY OF HEARING

Voter Privacy: An overview of information practices nationwide and California's process. The Task Force heard testimony regarding background on what California does to keep information private and where it falls short.

The threshold for casting a ballot is registering to vote. Public confidence in the confidentiality provisions of the Elections Code is integral, then, to ensuring the maximum participation of citizens in the electoral process. Encouraging voter registration and ensuring maximum participation is a statutory obligation of California's elections officials pursuant to Elections Code Section 2103.

Nationwide Overview

The voter registration process used by California and other states varies. Each state uses different standards to determine what information is to be gathered and what notice and instructions are provided to voters. This notice facilitates understanding of the process, and whether access to the data is permitted to any "secondary users," in addition to elections officials. California and other states have provisions for strict confidentiality for voters whose personal safety would be compromised if their personal information were publicly available. Finally, states have different standards on use of the information contained in the voter file by secondary users.

Kim Alexander, President of California Voter Foundation, provided an overview of a national survey on voter registration practices conducted by her organization. The study focused on these key issues:

- What data are being gathered on voter registration forms?
- What notice is provided to voters on voter registration forms?
- What data are added to voter registration records by election agencies?
- What data are kept confidential by election agencies?
- What secondary (non-election) uses of the data is permitted?

The findings of the survey include:

- Forty-six states provide a field for voters to supply a phone number; in 28 states, including California, providing a phone number is optional.

- Fourteen states, including California, ask voters for their place of birth.
- Thirty-eight states provide optional fields on voter registration forms, but voter notification that the information is not required was not as clear in some states.
- Only four states inform voters that their affidavit is a public record.
- Only one state, Iowa, informs voters of the potential for secondary use of the data.
- Eleven states omit from the public record all or part of the voter's birth date.
- Twenty-seven states offer an "opt-out" option for voters, so that their record is withheld from secondary users. [3]

Pursuant to these findings, the California Voter Foundation recommendations for California include:

- Adding voter notice on secondary use of data.
- Providing clear instructions to voters re: optional fields (what's really required).
- Limiting data collection—by determining if optional fields are really necessary.
- Restricting secondary distribution of sensitive data—date of birth, place of birth, etc.
- Ensuring database security—in May 2002, the State Controller's database was hacked and illegal access was gained to records of 260,000 state employees.
- Ensuring security for Internet voter registration to prevent unwanted access.
- Strengthening parameters on the prohibition on commercial use of the voter file.

According to Ms. Alexander, the Fair Information Principles used by the Federal Trade Commission should be applied to voter registration data:

- Choice—withhold certain data for secondary use; allow voters the choice of how they might be contacted by campaigns (mail, telephone or e-mail).
- Notice—explain to voters who gets access to the data.
- Access—voters should be able to request from government an accounting of the data government has on file.
- Security—assurances that the data is protected.

The Task Force found that additional principles from the Organization of Economic Cooperation and Development Fair Information Principles would be useful to consider as well, including:

- Limitations on collection of data.
- Specificity on purpose and use of data gathered.
- Accountability for safeguarding the data.

Voter Registration in California

There is not one voter registration form used in California—there are more than 58, at least one for each of the 58 counties in addition to the Secretary of State's form and a national form. Each

[3] See Appendix C for a complete copy of California Voter Foundation President Kim Alexander's testimony

county is free to modify the forms that they use, and some do. In some counties, voter registration forms are provided in multiple languages. The National Voter Registration Act of 1993 forms used by the Department of Motor Vehicles and by social services offices are also available to voters. But even the standard information required on all forms—such as birth date—is controversial.

State law now requires that voters be asked to voluntarily provide their ethnicity pursuant to AB 587, (Chap. 385, Statutes of 2003). A new federal law, the Help America Vote Act of 2002 (HAVA), also requires the state to collect driver's license numbers or partial Social Security numbers for all registrants beginning January 1, 2006.

The terms used in the law pre-dating both AB 587 and HAVA to characterize permissible uses of voter data are very broad, and sometimes there is a blurred distinction between what use is allowed and what is not. Hypothetical examples provide an illustration: Does a business requesting the voter file to contest a zoning decision that will affect its ability to build a store constitute a legitimate political use, or is it a prohibited commercial use? "Skip tracers" who are searching for "bail jumpers" have not been viewed as legitimate government users without a court order. And political consulting firms that do not yet have a dient (a campaign or candidate) are often denied access to the voter file.

The varying degrees to which information is gathered on different forms and the need for discretion and interpretation of the broad definitions provided in law are difficult issues that state and local elections officials confront.

Recommendations to improve enforcement and voter notice include:

- Allow for "salting or seeding" the file with fictitious names, which could assist in uncovering improper uses of the voter data in commercial mailings.
- Provide explicit authority for penalties in statute, which would alleviate any potential challenge to the existing penalties in regulation.
- Simplify the voter registration form, which would facilitate discussion about the need to include personal information on the form for election purposes, including whether any of that information should not be collected.

HEARING # 2 - November 12, 2003—San Diego, California

KEEPING FORMS AND DOCUMENTS PRIVATE

Testimony at this public hearing was provided by:
Sally McPherson, San Diego County Registrar of Voters
Jim Wisley, Consultant to then-Speaker Herb Wesson
Jerry Mailhot, Political Petition Coordinator
Bill Wood, then-Senior Attorney for the Secretary of State's Elections Division
Lisa Weinreb, Director, High-Tech Crimes Unit for San Diego County
Joanne McNabb, Director, California Office of Privacy and Protection

SUMMARY OF HEARING

<u>Why is Voter Privacy Important?</u>: Collecting voter information and the potential for misuse of data. The Task Force heard testimony about issues related to voter information provided on forms (such as initiative petitions, voter registration cards, provisional ballots in a recount, etc.) What types of access should be provided for this information? How is this information handled? What kind of notice is provided to voters?

Collecting and Handling Voter Information

County Registrar's Offices provide voter registration forms for use in individual counties. Forms are distributed at elections officials' offices, at other government offices, at schools, at the DMV, to campaigns and candidates, and to voter registration drives. As many as 10,000 registration forms per day are requested and distributed at larger counties.

These forms ask for personal information that for certain voters may include their driver's license number or partial Social Security number. County elections offices track the voter registration affidavits distributed, and technological innovations help counties know how many forms come back from each party who received the affidavits. If a voter does not mail back their forms directly, any third-party registrant involved in registering the voter must sign the affidavit personally and deliver it within 36 hours to the Registrar. Any violations of this legal requirement are reported to the District Attorney.

In San Diego County, 1.25 – 1.4 million voters are registered at any given time. Voter files are on a secured network that is not available online. The voter file is confidential, but access is provided to campaigns and for government use, or scholarly, legal or journalistic use. Before 1995, anyone could request this info, but the law has been changed to restrict access since then. Driver's license and Social Security numbers are always confidential pursuant to the Government Code. While Judges' and District Attorneys' voter file information is usually kept confidential, their addresses become public if they run for office.

While complaints and violations are referred to the District Attorney, these complaints are not always met with satisfactory results. An individual complained that he received junk mail with

the same misspelling that appeared in his voter file, but there was no investigation or prosecution. It was unclear why this case was not prosecuted, but it appears as though investigative and prosecutorial resources face competing demands that may be given priority, particularly violent crimes and property crimes.

Private, Third-Party Collection of Private Information

In addition to county elections offices, paid signature gatherers for ballot measures often register voters at the time they circulate petitions. Only the signature of a registered voter is counted when determining the number of valid signatures on petitions, but a person who signs a petition may also simultaneously register to vote. Firms that hire petition signature gatherers are interested in safeguards that protect against forgeries and fraud in the petition signature gathering process. But some argue that there is a built-in incentive for fraud because the amount of money earned by signature gatherers is typically based on the number of signatures or voter registration affidavits they submit. Undetected false or fictitious signatures and voter information will generate income. (See also San Francisco hearing, November 21, 2003 for additional information on enforcement issues.)

To mitigate this potential, some groups that fund voter registration and signature gathering efforts pay on a full-time, hourly basis, instead of paying seasonally on a piecemeal basis for each new voter registered. They report some success in minimizing substantially the number of "bad actors." Other recommendations to reduce fraud include:

- Improving the "signature gathering culture," which often has relied on individuals with criminal convictions in the employee pool.
- Mailing postcards to registrants to see if any are returned as incorrect to detect errors or fraud.

The consequences for misuse or mishandling of voter information are potentially serious.

Identity theft is the fastest growing crime in America. [4] Nearly 10 million people across the nation were victimized last year. Losses to businesses and consumers totaled more than $50 billion. It can take years for a victim to clear his or her name. Currently, there are virtually no proactive, preventive programs for identity theft. Law enforcement is hampered by the difficulties of pursuing perpetrators across city, county and state lines, and victims are concerned that police don't take the crime seriously enough. Most of those who are victimized don't realize it has happened until well after the fact and a loan is denied, or they find out about crippling debt that is ruining their credit report. A driver's license number or a Social Security number can be enough to commit identity theft.

In later discussion, Task Force member Beth Givens noted with concern whether inclusion of place of birth on the California Voter Registration Affidavit made California voters more susceptible to identity theft. She recommended that it be removed. Givens explained that if an identity thief were to illegitimately obtain voter records, they would know the individual's date of birth, which is vital to the crime of identity theft. And then with *place of birth* available on the

[4] See Appendix D for copy of California Office of Privacy Protection Overview

voter record, it would make it easier for the thief to gain access to a birth certificate and obtain additional information that is useful in stealing someone's identity. As Givens explained, the data elements of a voter record, in the wrong person's hands, essentially comprise an "identity theft starter kit." The only other data the thief needs to complete the starter kit is the Social Security number, which is relatively easy to obtain through other means.

Court Decisions that Undermine Statutory Confidentiality of Petition Signatures

There is also a recent trend that may undermine the reserve right of voters to petition for changes through ballot measures because it creates the potential for voter intimidation.

The signatures and voter information contained in ballot measure petitions are statutorily defined as non-public and confidential documents within the Public Records Act (Government Code Section 6253.5). Two trial courts, one in Sacramento and another in Los Angeles, appear to be breaking down this definition. The statute allows recall, referendum, or initiative petitions to be examined by proponents to determine why elections officials disqualified signatures. Other governmental agencies, including the Secretary of State, may only examine petitions after obtaining an order from the appropriate Superior Court. But there is no provision in the law for opponents to examine the petitions. Despite that fact, these two trial courts have permitted opponents of measures to not only examine, but copy petitions, one for a recall and the other for an initiative, based on the argument that some relevant information might be revealed.

There are ways to establish whether any improprieties have occurred that do not require the release of individual names of petition signatories. The political process allows for anonymity (such as the secret ballot) to ensure that voters are free from intimidation to exercise their franchise rights. If an employer discovered that an employee had signed a petition promoting a ballot measure that the employer viewed as contrary to their business interests (such as requiring a living wage or preventing expansion of a manufacturing plant), the employer might retaliate by firing the employee. These court decisions fail to recognize these potential issues for which these principles act as safeguards.

To address this situation:

- Standards could be placed in statute for non-proponents' examination of petitions, with legislative recognition that the harm of disclosure most often outweighs the benefit.
- Mandated in-camera review of petitions by judges could be used as an alternative to opponents' review.
- Protective orders could be mandated when petitions may involve employees of the opponents of a measure.

HEARING #3 - November 21, 2003—San Francisco, California

CONFIDENTIALITY ISSUES AND ENFORCEMENT OF CURRENT LAWS

Testimony at this public hearing was provided by:
Thomas Newton, Legislative Advocate for the California Newspaper Publishers Association
Kathleen Krenek, Director, Next Door, Solutions to Domestic Violence
Tim Fries, Government Affairs Director, California Union Safety Employees
Ric Ciaramella, Chief Investigator, Secretary of State Elections Division
Susan Oie, Deputy Attorney General

SUMMARY OF HEARING

Balancing Openness and Privacy of Voter Records:—Competing interests. The Task Force heard testimony addressing whether certain classes of people (such as elected officials, peace officers, battered women, etc.) should be granted confidential voter registration status. Should elections officials keep such people off of the voter file? What is being done to enforce laws regarding protecting voter data? Are current state voter privacy laws being enforced?

Every democracy that is legitimate is accountable for the results of its elections. This requires a certain transparency to the process, including understanding and creating the ability to confirm the eligibility of candidates and voters. However, there are times when an overriding personal interest in public safety requires voter anonymity—beyond that provided by the secret ballot. Courts have generally upheld the right to that confidentiality. California law creates a balance between these competing interests by maintaining confidentiality for voters' personal information when it comes to the public generally, but also allows certain classes of people access to the voter file—the four exceptions: scholarly, journalistic, political or governmental purposes.

Journalists tend to use the voter registration file in ways that are similar to political uses. They use voter registration files to:

- Determine candidate eligibility (A state legislative candidate and many local candidates must be registered voters in the district they intend to represent).
- Evaluate redistricting proposals by the legislature and others (These plans must meet standards to ensure fair representation).
- Establish a subject or source's "identity" (Are they who they claim to be?).

Journalists support public policy that denies access in the case of demonstrated "bad acts," but they argue that policies must be weighted toward public access unless public interest in *denying* access clearly outweighs the interest in *granting* public access. The ultimate safeguard is that misuse of these records is a crime.

Notwithstanding the broad definitions of the purpose or use allowing access to the voter file, more precise definitions of "journalistic uses" would be difficult to achieve. The First Amendment is broadly construed, so that anyone with paper and a mimeograph machine has

traditionally been considered a journalist. Today "bloggers" (those that use the Internet to disseminate information) are considered journalists—and some recognized journalists use "blogs" extensively. The "saving grace" of the current system is that a person must sign their name and state their intended use of the voter registration file when they request it. If they do so fraudulently, that is a crime. Licensing the press is not realistic or desirable, so a signature and affidavit must be sufficient.

The commercial use restriction is relatively new and should not be confused with the well-founded access granted to the press. Furthermore, voters are participating in a (newsworthy) public process when they vote. Jury service presents an analogous situation. People cannot opt out of jury service, however (while they can choose not to vote). But the decisions made by jurors are presumed to be protected information because it protects the integrity of the judicial process. Voting is a public process up until the time the curtain to the polling booth is drawn. (The meaning of this entire paragraph is unclear)

There are situations, however, when the law recognizes the overriding interest in personal safety of voters. Battered women's advocates often contest the "public interest" doctrine on open records because they advocate for the personal safety rights of victims. The Safe@Home program (an address confidentiality program that includes confidentiality for voter registration data administered by the Secretary of State's office) is a statewide program that many consider underutilized. Victim's advocates say that more than ever, address confidentiality is necessary to help victims—to live in safety from their abuser. Batterers are obsessive—their tenacity is the cornerstone of their existence, and they will check DMV, Social Security and other sources of government documents to track a victim. The Internet is a new source of information.

About 80% of women are victimized after they leave or consider leaving an abusive relationship. Whole families can end up dead if an abuser locates them. The practical reality is that only 4-10% of victims enter protective programs. Early concerns that an address confidentiality program would be used as a means to evade bill collectors, or for other inappropriate uses, have not materialized. By contrast, personal stories provide examples of what must be surrendered by victims of abuse to escape violence—giving up educational degrees, family associations, community life, religious affiliations, and voting.

Domestic violence cuts across all income, race, creed and religious demographics—and as many as 50% of women will be battered sometime during their life by an intimate partner. The solutions are not impossible—even the U.S. Postal Service has developed a way to keep change of address information confidential. Voter registration confidentiality is a part of that need. It allows a person the opportunity to participate in the democratic process without surrendering personal safety.

Law enforcement personnel are in need of confidentiality at times to prevent retaliation. Anecdotal information suggests that it is needed on a case-by-case basis: A code enforcement officer from the Department of Food & Agriculture who had to exterminate ducks and chickens that had contracted New Castle's disease to prevent its spread to other fowl was targeted by the animals' owner. The animals that were exterminated were family pets. The animals' owner used voter records to find the officer's home address, took digital photos of the officer and

posted signs publicly accusing the officer of "murder." However, removing all peace officers in California from the voter rolls would mean a loss of several hundred thousand records.

There is a general concern that the ability to access the voter rolls with a promise that "I am not a liar" may not be adequate. Law enforcement officials suggested that elections officials could notify persons whose individual records have been requested. A request for a single, individual record may be an indication that a person is being "targeted," whereas requests for aggregate data suggest an analytical or political purpose for gathering the data. However, it was noted by Task Force members that any access for voter file data, even for a single record, could only be gained through a state-mandated application process. That application process is only available to those who are eligible to gain access to voter records (journalists, scholars, political users or governmental users).

Finally, there are specific instances where a user might request access to only one record, such as when a journalist is attempting to independently establish a candidate's identity and eligibility to seek office from voter file records. More rigorous standards for identifying persons who request the voter file could be established. Presently, elections officials take at "face value," the claim from an applicant that they are, indeed, who they claim to be and that they are among the four classes of exceptions: scholarly, journalistic, political or governmental purposes eligible to receive the data.

Restrictions in state law—a prohibition on commercial use and the validity of an overriding interest in personal safety—have been upheld by the courts.

Elections officials testified that they reject attempts to gain access to the voter file for commercial purposes. In the most recent significant case, a commercial vendor had attempted to argue that voter registration was the same as "any other record" gathered by government. The vendor argued that the exceptions to access provided in the law were not valid. The vendor proposed that the records should be accessible for commercial use and resale. The court rejected that argument, in part, because the Attorney General successfully argued that the exceptions provided for in California law had specific purposes (IRSC v. Jones). The arguments for journalistic access provided earlier, for instance, were contained in a deposition from a journalism professor from USC.

In addition to Elections Code sections, the Information Practices Act of 1977 articulated standards and reasons for keeping the data private. These sections of law contain the provision that they apply "notwithstanding any other provision of law," suggesting that they supersede the Public Records Act provisions, which provide for public access to government records.
The statutes work together to keep secure information that should be private—names, addresses and other personal information. Elections Code Section 2166.5 protects the names and addresses of domestic violence and stalking victims, for instance. Originally, the law was intended for judges, district attorneys, and public defenders. This information would never be seen, even under the exceptions granted to the four secondary users because it is confidential. This confidentiality exists independent of the four exceptions: scholarly, journalistic, political or governmental purposes that apply generally to the voter registration file, which contains names of persons who have not been granted confidentiality under other sections of law.

Investigation and Enforcement of Voter Privacy Allegations

The Secretary of State's Office investigates cases related to voter fraud, petition fraud and misuse of the voter file. Cases presented to District Attorneys have helped secure 44 convictions in the past eight years that resulted in cumulative sentences of 15 years in state prison. The commercial use prohibition on use of the voter registration file, however, is a misdemeanor.

There have been 18 cases of violations of Elections Code Section 18109 investigated in the past eight years, but no case has been prosecuted under the statute. A high-level prosecution of such a case might serve as a deterrent to abuse. Although investigators as criminal matters pursued the cases involving commercial use and sale of the information over the Internet, the cases were adjudicated as civil matters. The Secretary of State's investigative unit has seen two large cases in nine years. Other cases of privacy have arisen—such as a campaign opponent who gathered all the personal data available on a candidate and posted it on the Internet. This is unnerving, but not illegal.

The lack of prosecutions of these violations stem, in part, from the broad definitions for the four exceptions: scholarly, journalistic, political or governmental purposes. A lack of knowledge on the part of prosecutors about the law and competing demands on district attorneys' time to address other criminal matters may also contribute to the relatively low number of prosecutions.

Sometimes, what appears to be a suspicious activity turns out to be perfectly legitimate. For instance, a person representing himself as a freelance writer contacted the Secretary of State's office to ask extensive questions about how to gain access to voter data from the County of Los Angeles. There is no way to verify a person's status as a freelance writer. And the questions appeared to be aimed at finding a loophole to gain access to the data for an inappropriate use. But, ultimately, this request was legitimate—the piece he was writing ran in the Los Angeles Times.

There is anecdotal evidence that there is a "bounty hunter" (paid signature gatherer) problem in the voter information gathering process. A woman approached at a supermarket filled out a voter registration card. Days later she was contacted by the person who had collected the information. A database of 1,000 bounty hunters was searched and the person was registered there. A further background investigation revealed he was also a registered sex offender.

In the experience of Secretary of State investigators, many bounty hunters have a criminal record. Additionally, recent federal court decisions upheld the rights of bounty hunters to participate in the signature-gathering process. When District Attorneys understand the laws, they are more willing to prosecute and more successful when they do. Stiffer penalties for violations by paid bounty hunters might also help encourage more vigorous prosecution because serious penalties show that the Legislature and the public consider this a serious offense. Laws that require paid signature gatherers to report to local registrars, show identification and fill out a form would be helpful for purposes of enforcement.

In five years, the issue of privacy is likely to become an even bigger issue because of the growing sophistication of the Internet.

HEARING #4 - December 15, 2003—Los Angeles, California

THE VOTER FILE – ACCESS AND PRIVACY

Testimony at this public hearing was provided by:
Lorraine Patterson, Representative, Los Angeles County Registrar
Bob Smith, Deputy Registrar, Santa Barbara County
Steve Rodermund, Orange County Registrar
Bob Proctor, Representative, Statewide Information Systems
Shellie Garrett, Representative, Voter Contact Services

SUMMARY OF HEARING

Access to the Voter File for Vendors (and others): The Task Force heard testimony regarding specifics from different county elections officials about what they do to assure privacy – and requests they receive for which they need guidance. Testimony concerned access by vendors to the file and whether the law prohibiting nonpolitical commercial access is too limiting or not limiting enough as well as how sensitive voter data is controlled and protected?

The broad definitions of allowable use of the voter file (journalistic, scholarly, political and governmental uses) create ambiguities and "gray areas" in the law. Controversy and dispute will arise even when there is a well-established process and procedures and even where there are experienced elections officials and professionals who understand the law.

Voter registration is critical because it is the start of the whole voter participation process. The laws on the subject are seemingly contradictory—on the one hand the information is confidential, on the other hand access is explicitly granted in the law. The demand for this information has exploded in recent years. There is a much greater capability to provide the data because of the ever-advancing capabilities of information technology and the ever-decreasing costs of data processing. By the same token, there is a much greater capability to manipulate and use the data by those who receive it. Sometimes these advances in computer technology strain the confidentiality provisions of the law.

The process used by counties to manage sale and distribution of voter data is straightforward. County elections officials and vendors receive the same training course to educate them both on the process and the rules governing use of voter data.

Those who purchase the voter file are first advised that confidentiality is a part of the law. Then an application is provided that includes fields for the name, telephone number and address, including a business address, of the applicant. The form also requires that the applicant provide a stated purpose for the data. County elections officials attempt to make sure the applicant understands what purposes are allowed under the Code. The application is signed under penalty of perjury (Elections Code Section 2188).

Despite these attempts to create a well-articulated and well-understood policy and procedures, conflicts still arise because access to this data is highly desired. More applicants are requesting the data, and new applicants are requesting the data as technology makes it possible to use this data more easily.

Technological advances have led to an explosion in the number of requests for the data because elections officials can format the data in multiple ways and users can use the same technology to manipulate the data more easily.

Voters call elections officials almost daily to criticize the release of the data, but again there is a seeming contradiction: Both confidentiality of voter information and right of access by certain parties are explicit in the Elections Code.

There are many different types of requests for information contained in the voter file: absentee voter information, voter history information, street indexes, and other combinations of requests. As Election Day draws nearer the electrons office is bombarded with requests. Any perceived violations of the rules governing the appropriate use of the voter file are referred to the District Attorney for follow up. A county registrar's office is not a regulatory or enforcement agency. Allegations are referred to District Attorneys.

Every request for purchase of the voter file must be made via an application, which is required by law. Some counties maintain a list of recognized purchasers.. Government agencies are allowed to apply annually. In some counties, every purchaser of the voter file must provide credentials of some sort, proof that the buyer represents the entity that they claim to represent. The public can view the voter file in the Registrar's office, but the "personal information" specified under the Government and Elections Codes is redacted from this file, including the person's home address, telephone number, birth date and political party affiliation. The only persons with access to the complete file are state and county elections employees, city elections employees and the county's election-services contractors.

Despite the guidance provided in the law, there is a lack of uniformity among the counties regarding treatment of purchasers of the data file. The definitions contained in the Elections Code that specify access to the file are broad, and county elections officials generally believe they need more specificity. As administrators of the law, they express an interest in minimizing discretion. Elections officials ask questions when applicants seek access to voter data to determine the applicant's needs and the applicants intended use of the data. But elections officials must accept this information at face value. It would be infeasible for elections officials to verify the truth of the information provided by the applicant, especially when the information on the application is submitted under penalty of perjury.

At times, the largest volume of voter complaints about the misuse of voter registration file data is about the use of the data by campaigns, which is a legitimate, legal use of the data. When cases warrant additional attention, the cases are referred to the Secretary of State for investigation.

Allegations about misuse of the voter file are relatively few, compared with the more numerous legal disputes related directly to elections. Many more cases are filed over candidates' ballot

designations, or disputes over ballot measures, and these cases absorb resources that are already stretched thin. For example, nearly 30 lawsuits were filed contesting various aspects of the October 7, 2003, Gubernatorial Recall Election.

The lack of prosecutions related to misuse, especially commercial use, of voter file data may not necessarily indicate that no such abuses have occurred. Rather, it may be related to a lack of systematic strategies to detect the use or misuse of data -- strategies, such as "seeding" or "salting" the file with unique names that would enable officials to trace abuses back to a particular user. Tracing misuse of voter files is also hampered by the common process of mingling data from other sources, as well as sorting the data into different formats and for different purposes, ultimately making it impossible to determine where the data originated. With the addition of magazine subscriptions lists, membership lists from interest groups (e.g. National Rifle Association), and gender or ethnicity attribution lists to the voter registration file, the origin of the data becomes indistinguishable.

County elections officials are also concerned about the new, personal data that is to be collected from voters under the federal Help America Vote Act of 2002—driver's license numbers and partial Social Security numbers.

The ability of elections officials to anticipate or react to allegations of misuse is limited. It does not appear as though any elections officials are "seeding" the data files with fictitious names as a possible tracing tool to detect violations. And some elections officials believe they have no ability to restrict access to the data, even if they believe it may be or has been misused. The law only provides that the stated purpose must fall within the parameters of one of the four allowable uses: scholarly, journalistic, political or governmental purposes.

Elections offices are not investigative units, so it is difficult to judge the appropriateness of when and how to take punitive steps. Allegations of misuse are referred to the District Attorneys' offices. Allegations of voter data misuse must compete for the "attention" of District Attorneys who have jurisdiction for prosecution of all criminal matters in the county. One difficulty in investigating and prosecuting misuse of voter file data is the difficulty in proving intent to misuse the data.

It is easier to administer the law when the purpose of the statute is clearly stated, some elections officials argue. And it is worth noting that the Legislature has made policy distinctions about public disclosure based on technology. For instance, campaign finance reports available via the Internet have some of the data redacted. The home address and phone number of campaign donors and campaign treasurers is public information, and is provided on paper forms, but when the information is displayed on the Internet, the law specifies that this information shall not be available on the "web." With the advances in technology, this same policy distinction might apply to voter data.

According to elections officials, ten years ago "daisy-chained," central computers stored the voter registration file data. The prevailing attitude at that time was that the information was primarily for internal, election use. Information technology has evolved into a decentralized, PC-based system linked to networks. The Internet, websites, CD burners and other high-tech

innovations have proliferated. The software products and peripherals now exist to manipulate large amounts of data. This has led to an explosion of requests based on technological advances in computer equipment and the ability of people to use them as tools.

Technology also enables elections officials to create data files that suppress information (i.e. redaction). Elections officials have the ability to eliminate any field of data on the voter registration form, and vendors often segregate data they receive in the voter registration file because it is not needed for their purposes. However, county elections officials warn that they are overloaded now. If elections officials must continue to gather more and more data on voters and then create programs and policies to suppress that data, at some point it becomes overwhelming. This can lead to policies that are unworkable, prohibitively expensive or infeasible to implement. Confidential files, for instance, show up nowhere in electronic data files; they are handled manually, and only a select few (usually one or two people) know about them and can access them. The number of these files ranges from several dozen in a medium-sized county to several hundred in a large county.

Data Vendor Purchases of the Voter File

Data vendors perform services for all types of clients—government agencies, providing aggregate data to scholars, and a large amount of political work. Many firms have websites where the public can see the kind of aggregate data the firm has or can obtain. Most firms do not provide any detailed information over the Internet to clients. Vendors typically know who their potential customers are: the identity of candidates (from candidate filings), legislative members, PAC's (Political Action Committees) or Independent Expenditure Committees that request services.

Voter file information is also routinely requested and provided to members of Congress for "franking" privileges to send mail to their constituents. By and large, the law and the process used by counties allow vendors to conduct their business. But the needs of clients who have legitimate access to voter data can be immediate. Clients request and expect that specialized voter lists, or voter call sheets, be provided virtually upon request. The immediate needs of the client do not accommodate the time it takes for vendors to obtain the voter file data from the counties.

Vendors typically provide specific products to candidates, consultants and politic parties: lists and labels. The vast majority of the work product is "targeted" (data that is sorted by criteria and used to send specific types of mail to specific voters). Vendors try to enhance the voter file with other information, including the National Change of Address list (to remove inaccurate addresses); gender is added to the list of data; there is a quasi-ethnicity dictionary software program that can be applied; and they "household" the data for mailing purposes (to eliminate multiple mailings to different members of the same household).

A hypothetical example of a client is the proponent of a local school bond measure. The first step is polling to determine public strength of garnering a two-thirds vote on the measure. The polling list might be generated by a vendor using the voter registration file to determine the electorate (eligible voters) demographics and high propensity voters. On the basis of that

information, labels for mailings and lists for walking door-to-door to campaign are generated. A list of voters who vote by mail might be generated. Data would be used to identify likely voters and likely supporters. In addition to the voter's personal data, the three primary/immediate needs for data are the party affiliation, the voter's gender, and the voter's age. Voting history and absentee voting propensity are also used frequently. Commercial vendors approach data vendors. But with confidentiality mandated, vendors sign a form under penalty of perjury stating a (non-commercial) purpose and acknowledging the prohibition on commercial use. The forms available now do a good job of informing the vendor of these requirements.

Vendors believe that the new elements required by federal law on the voter registration affidavit—the partial Social Security number and driver's license number—have no political purpose. The place of origin/birthplace of voters requested on the California voter registration affidavit is useful to garner data on ethnicity at times, but that information can also be obtained from Census data. Date of birth is of interest to members of Congress. They want to talk to senior citizens about senior issues, for instance. They wouldn't want to send a mailing to a younger person about Medicare changes.

Once data leave the hands of the vendor (who collates and sorts data), however, it is not tracked. It becomes the property of the client—candidates, campaigns, elected official or political parties. A data vendor might not get the voter registration file directly from elections officials; they may be getting the lists from clients who fall into one of the four categories for legitimate access. There is no explicit prohibition on the reuse of the list, so the data received from a client might be retained and packaged for sale to other clients for those purposes allowed under the law. Vendors often provide notice to clients that the information can only be used "for these purposes," but there are gray areas sometimes.

Arizona law does not provide for sale of the voter file, but the law also requires that the voter file be provided to the political parties on a quarterly basis. The parties provide it to the vendors who contract with them. This is used to build a statewide database.

Regardless of the rules that prevail in the various states, there is a tendency to create an on-site database using information provided by the vendor that is used exclusively by campaigns and by candidates. Those who testified said that vendors have no control over the data any more. Vendors could sign an agreement to track the data, but they claim it would be very difficult to judge where the data come from and how the chain was broken.

Confidentiality for vendors tends to mean confidentiality for the client. Clients request data in certain ways—creating sub-files of data. There is also data from other sources being added. For instance, the National Do Not Call Registry could be added, so what is compiled becomes a unique list that the client owns.

Vendors believe, however, that there are ways to limit access to the data, while still using private contractors. For instance, the U.S. Postal Service has created a process for using a select group of data vendors who have access to the National Change of Address information.

Elections officials generally acknowledge that the established data vendors that they interact with on a regular basis tend not to be "a problem."

One other potential "gray area" of the law exists when it comes to public records. A vendor created a database of registered voters in legislative districts to the one house of the Legislature for constituent contact purposes. It is unclear whether this database could be construed as a public record subject to a Public Records Act (PRA) request. Any person might be able to request it under the PRA, even if they do not fall under one of the four exceptions: scholarly, journalistic, or political purposes, or for governmental purposes. The data may be suspect. It may be three or four years old, but if the purpose is commercial, the potential user may not be as concerned about that. This could be a serious loophole. In fact, data purchased by members of Congress are actually the property of the Congress. In theory, these data files could be subject to a Freedom of Information Act request.

Public testimony submitted by J. Blair Richardson, General Counsel and Chief Privacy Officer, Aristotle Publishing, December 29, 2003.[5]

[5] See Appendix E for a copy of public testimony submitted by J. Blair Richardson, General Counsel and Chief Privacy Officer, Aristotle Publishing

Task Force Recommendations

Under current law, personal information contained in the voter registration file is generally confidential. The law provides further protections for certain classes of persons when there is an individual interest in privacy for reasons of personal safety that supercede the public interest in access by anyone other than elections officials or law enforcement personnel. Commercial use of the information is explicitly prohibited.

For purposes of openness and accountability, to further our understanding of how the electoral process "works," to encourage participation by informed voters, and to further other governmental purposes, access to the voter file is provided for: scholarly, journalistic, political or governmental purposes.

The Task Force makes the following recommendations:

1. Notify Voters About Secondary Uses of Voter Registration Information.

This recommendation is intended to provide voters with more notice about the availability of voter file data to a select group of secondary users (journalists, scholars, those involved in the electoral process such as candidates, ballot measure campaigns and political parties) and to provide more notice to a select group of voters who may need and request strict confidentiality of this data.

The contents of the Voter Registration affidavit are prescribed by law (Elections Code Section 2150). The Task Force recommends the Secretary of State sponsor legislation to accomplish the following:

- Add the following statement to the Voter Registration affidavit instructions, and replace an existing statement on the Registration Form Receipt (the tear-off section of the Voter Registration Affidavit) with the following statement:

  "Confidentiality of your personal information, including your home address, may be obtained for domestic violence or stalking victims, reproductive health care workers, or others. For more information call ((877) 322-5227) or contact the Safe at Home program at (www.ss.ca.gov/safeathome/.)"

- Include the following statement on election-related websites hosted by the state and counties, in the state ballot pamphlet produced by the Secretary of State, and, if possible, in sample ballots produced by county elections officials (i.e. the legislation recommended should make the placement of the statement below in local sample ballots permissible, not mandatory):

  "Information on your voter registration affidavit will be used by elections officials to send you official information on the voting process, such as where your polling place is located, and which issues and candidates will appear on the ballot.

Commercial use of voter registration information is prohibited by law and is a misdemeanor. Voter information may be provided to a candidate for office, a ballot measure committee or other person for election, scholarly, journalistic, political or governmental purposes as determined by the Secretary of State. Driver's license and Social Security card numbers cannot be released for these purposes. If you have any questions about the use of voter information or wish to report suspected misuse of such information, please call the Secretary of State's Voter Protection and Assistance Hotline: (800) 345-8683."

Certain voters, including stalking or domestic violence victims, reproductive health care workers, or others who face life-threatening situations, may request that their voter information remain confidential and not be released for the purposes described above. For more information on these programs, please contact your local elections official or the Secretary of State's Safe at Home program at (877) 322-5227, or visit the website at www.ss.ca.gov/safeathome/."

- Include on the voter notification card (Elections Code Section 2155) the following statement:

  "Confidentiality of your personal information, including your home address, may be obtained for domestic violence or stalking victims, reproductive health care workers, or others. For more information call ((877) 322-5227) or contact the Safe at Home program at (www.ss.ca.gov/safeathome/.)"

2. Identify More Clearly Optional Information on the Voter Registration Form.

This recommendation is intended to clarify for voters that certain personal data is not necessary to complete the voter registration affidavit, so that they may make a more informed decision about what data they would like to provide to elections officials and select secondary users. This recommendation does NOT extend to the voter's option of choosing a political party affiliation.

The Task Force recommends the following:

- Identifying in the actual fields on the voter registration form where voters provide the data, not just in the instructions, what information is optional (not necessary for the voter to complete to become a registered voter) by adding **"(Optional)"** in red type in the field on the affidavit, excluding the field in which voters mark a preference for political party affiliation.

- Reformatting the instruction for the affidavit so that the word **"(Optional)"** appears, in red type, at the beginning of item 8 (telephone, e-mail), as follows:

  8 TELEPHONE: (Optional) Please include area code. This number will help elections officials contact you and are posted in precincts on Election Day.

  E-MAIL ADDRESS: (Optional) No person shall be denied the right to register to vote for failure to furnish an e-mail address. Every character including dots, dashes, slashes, and underscores should be in a separate box.

This policy should also be applied to the new requirement (effective January 1, 2004) that the voter registration form request that voters voluntarily provide their ethnicity on the voter registration affidavit.

3. <u>Clarify Voter Registration Requirements.</u>

This recommendation is intended to clarify voter registration requirements pursuant to the Help America Vote Act of 2002 (HAVA), and to ensure that voters understand what information must and can be provided.

As the Secretary of State implements HAVA, it will be critical to take all necessary steps to alleviate the privacy concerns of voters and prevent identity theft, especially with respect to maintaining the confidentiality of and redacting driver's license numbers and partial Social Security numbers. We note that election laws already have been modified to help accomplish this purpose. (Government Code Section 6254.4 (c) [collection of driver's license numbers, California identification card numbers, Social Security numbers and unique voter identification numbers for the purposes of complying with HAVA shall be "confidential and shall not be disclosed to any person."].) Finally, the Task Force urges the Secretary of State's HAVA Advisory Committee to study all voter materials to ensure they provide adequate notice to voters about the new HAVA provisions.

The Task Force recommends the Secretary of State sponsor legislation to accomplish the following:

- To the extent feasible, make it clear those federal requirements to provide a driver's license number or a partial Social Security number are not misconstrued as a requirement to provide both. To address this: ensure that all voter registration cards request the driver's license number as the first option for the voter, and place in capital letters and red type the word "OR" between the fields for the driver's license number and partial Social Security number.

- Because the Social Security number is more sensitive personal information and makes a person more vulnerable to identity theft, research the legal obligation to request a partial Social Security number and exclude requesting the information on the voter registration affidavit if at all possible.

- Consider placing the instructions for completing the voter registration affidavit at the "top" of the voter registration card. Currently, the instructions, including information about optional fields, is attached to the bottom of the affidavit, making it less likely that the voter, before they begin the process of completing the form, will understand what is required to complete the registration process and what is optional.

- The Secretary of State should consider these reformatting changes in the context of any larger effort that might be undertaken to simplify or otherwise improve the voter registration affidavit.

4. <u>Sponsor Legislation to Limit Uses of Voter Registration Data.</u>

The Task Force heard testimony from county elections officials particularly that the broad parameters for allowable secondary uses (journalistic, scholarly, political and governmental) provide minimal guidance about allowable uses. The current construction of the law is not explicit, but implies that personal use, in addition to commercial use, is impermissible.

To provide additional clarity, the Task Force recommends that the Secretary of State sponsor legislation that further defines these prohibitions, but also preserves the current access by secondary users as follows:

- Personal, private use of voter information data is prohibited.
- Reproducing and mass-producing voter file data on individual voters either in print, for broadcast or on the Internet is prohibited.
- Use of the data for the purposes of harassment is prohibited.
- Use of the data for voter contact for a purpose unrelated to journalistic purposes, scholarly purposes, political purposes on behalf of a candidate, campaign or political party, including surveys or public opinion polling; or other official governmental use is prohibited.

Further define "prohibited commercial use" of voter registration data to include, but not be limited to:

- Advertising products and services to consumers.
- Solicitation of consumers for products or services.
- Sales and/or marketing products or services to consumers.

Finally, the Secretary of State should survey "other government agencies" for the purpose of determining which agencies use this data, for what purposes, and to create parameters for its use by those other government agencies.

5. <u>Sponsor Legislation to Clarify Voter Privacy Best Practices and Uniformity.</u>

This recommendation is intended to ensure best practices and uniformity among the counties in the application of voter privacy policies.

The Task Force believes that current laws should be strengthened to protect against the impermissible uses of voter information, especially by secondary users. In addition, the Task Force believes voter information should be the subject of uniform retention procedures like those found in the Elections Code for similar voting documents (Elections Code Sections 17301-17306). Given existing law in these areas, any changes should be done through legislation.

The Task Force recommends that the Secretary of State sponsor legislation to:

- Require that applications for voter file data identify the "end-user" of the data; for example a scholarly use of the data might be identified with a specific university, or a political use might be identified with a specific ballot measure committee.

- Specify that reuse or resale of the data, even for a similar purpose, by another party is prohibited without further written authorization from the state or county elections officials from whom the voter registration file data was obtained.
- Require a retention and disposal procedure to safeguard the information while it is in the possession of the end user and ensure proper disposal of data when the end user discards it.

6. <u>Propose Legislation to Increase Criminal and Civil Penalties for Misuse of Voter Information.</u>

The Task Force heard testimony about the ambiguous nature of the investigation and prosecution of voter privacy statutes. Elections officials who testified said there is little conclusive evidence that California voter records have been used for purposes other than those prescribed in law. But Task Force members noted that such misuse is largely invisible, especially given that voter data files are not salted or seeded with unique entries in order to track misuse.

The Task Force believes tougher penalties may be appropriate to adequately protect against the misuse of voter information. This is particularly important given the ease with which electronic data files could be obtained by entities that do not have a legitimate right of access and then merged with other data files, thereby rendering them virtually impossible to trace.

The Task Force therefore calls on the Secretary of State to propose legislation concerning additional criminal and civil penalties for the misuse of voter information. Such legislation should address illegitimate commercial use of voter registration data as well as the misuse of strictly confidential voter registration data of domestic violence victims, stalking victims, reproductive health care workers and others whose data is protected under court order.

The legislative proposal suggested under Recommendation Number 5 could include a requirement that vendors employed by end users keep records on the use of data that includes, but is not limited to:

- Identifying the "end-user" of the data; for example a scholarly use of the data might be identified with a specific university, or a political use might be identified with a specific ballot measure committee.
- Prohibiting reuse or resale of the data, even for a similar purpose, by another party without further written authorization from the state or county elections officials from whom the voter registration file data was obtained.
- Requiring a retention and disposal procedure to safeguard the information while it is in the possession and when it is transferred to a client, and to ensure that voter records are properly discarded when they leave the possession of the end user.

The Task Force encourages the Secretary of State to study the feasibility of salting or seeding voter registration lists with fictitious names as enforcement and investigative tool for determining inappropriate or unauthorized uses of voter file data.

Finally, the Task Force recommends the Secretary of State to assess the investigative priorities for the enforcement division in light of the conclusions and Recommendations of this report.

Given the likelihood that this division's budget will not be increased during the current state budget crises, the Secretary of State should examine how the enforcement division's resources can best be allocated to respond to the Recommendations of this report, especially its ability to investigate misuses of voter data.

7. Ensure Secure Design of Statewide Voter Registration Database.

Pursuant to the Help America Vote Act of 2002, California will be required to create a single, statewide voter registration file, which will serve as the official list of voters for election purposes. The current number of registered voters in California exceeds 15 million people.

To protect against unauthorized access to this personal data, the Task Force recommends:

- The Secretary of State should integrate state-of-the-art security standards and best practices into the planning and design phase, and during construction and ongoing maintenance of the federally required statewide voter registration database, including ensuring that a threat analysis and risk analysis is applied to any design.

8. Safeguard Against Voter Intimidation in the Ballot Measure, Referenda and Recall Process.

Recent examples of practices relating to election challenges present the potential for creating a chilling effect on exercising the right to vote. Similar concerns apply to the rights of the people to exercise direct democracy, including the initiative, referendum and recall processes. Voters who cast provisional ballots might, inappropriately, be identified before the certification of election results, and opponents might identify petition signatories during a challenge to a ballot measure's validity. In both cases, voters might be subject to intimidation and coercion to "change their minds" about casting a ballot or signing a petition. The potential for a chilling effect on the electoral process should be eliminated.

Therefore, the Task Force recommends the Secretary of State sponsor legislation to clarify that:

- County elections officials are prohibited from releasing the list of provisional voters before an election is certified.
- The release of voter signatures contained on petitions seeking to qualify ballot measures, referenda and recalls is prohibited.

9. Require Additional Safeguards by Vendors Who Are Authorized to Use Voter Registration Information. *

The Task Force heard testimony from elections officials and data vendors regarding the unique relationship that these businesses have with both clients and elections officials. While not explicitly recognized in the Elections Code, data vendors are regularly employed by eligible secondary users (journalists, scholars, political entities and government) to sort, select, collate or otherwise modify voter registration index data to make it usable for purposes allowed under the law. Elections officials testified that in their experience vendors "understand and follow the

rules" and "are not a problem" when it comes to concerns about misuse of data and protecting voter privacy. The Secretary of State should accommodate this legitimate role in the process by allowing vendors direct access from elections officials to this data, while adding protections to the law that ensure that this practice is not abused.

The Task Force recommends that the Secretary of State sponsor legislation to:

Amend Elections Code Sections 2194 and 2188 to clarify and accommodate the reality that vendors are legitimately employed on a regular, ongoing basis by those who are entitled to access the voter file for journalistic, scholarly, political or governmental use. Any such amendments to the Elections Code should be accomplished in conjunction with a comprehensive approach to regulating secondary uses of voter information and enforcing voter privacy laws as provided for in recommendations number 5 and 6 in this report. Such access should be accompanied by additional safeguards by vendors that would include the following as a part of the application process used to acquire the data:

- Notarizing the vendor's application, in addition to providing the identification required under current law.
- Providing to the elections official a list of candidates, campaigns, political parties, officeholders and other eligible clients for which the vendor has performed services in the last three to five years—up to a maximum of 10 clients.
- Attesting to an affirmative statement that a court has never found the vendor, civilly or criminally, to have misused the voter registration index data in California or elsewhere.
- Providing to the elections official a copy of the vendor's process and procedures for screening clients to ensure that those clients are eligible secondary users;
- Providing a bond.
- Agreeing to regular and random auditing of any records, files or equipment by elections officials and law enforcement personnel.
- Agreeing to participate in any regulatory program designed to ensure the protection of private information, including salting or seeding the voter registration index with data unique to that company.
- Reporting regularly to elections officials on the use of the data on behalf of clients.
- Creating an enforceable promise not to resell or reuse the data for ineligible purposes.
- Specifying that violation of these conditions may include a fine and a denial of access to the voter registration index for a period of up to five years.

The Task Force did not agree unanimously on the above Recommendation:

Task Force Member Beth Givens abstained from voting on Recommendation Number 9, while the remaining six Members of the Task Force voted to adopt the Recommendation. Task Force member Givens' reason for abstaining from voting on Recommendation Number 9 is provided below.

Beth Givens Statement of Abstention on Recommendation Number 9:

"Although this Recommendation has some merit in my view, I do not support it at this time. I would like to see the effect of Recommendations 4, 5 and 6 before supporting direct access to voter data by commercial data vendors.

I am also concerned that the Secretary of State's enforcement resources may not be sufficient to adequately monitor and take action against wrongdoers, if a data vendor were to violate the provisions called for in this Recommendation. Before expanding the categories of entities with access to the voter files, I would like to see if the Task Force's
Recommendation on "seeding" or "salting" the voter files can be implemented successfully."

10. <u>Prominently Display Criminal Penalties for Theft or Removal of Voter Rosters at Polling Places. *</u>

Current law explicitly provides that at each polling place on Election Day a roster of names and addresses of those eligible to vote in that precinct be publicly posted and that a running tally of those who have voted be kept by poll workers and be publicly posted.

The Task Force had extensive discussion about whether the requirement for public posting of voters' names and addresses on rosters at each polling place represents an inconsistency in the Elections Code, which generally limits public access to this personal information. The Task Force ultimately determined that this seeming inconsistency was balanced by the Legislature against the use of this voter information by campaigns and candidates for the purposes of contacting voters to remind them to cast ballots on Election Day, an integral part of encouraging voter participation and ensuring a healthy democracy. (The meaning of the preceding sentence is unclear) However, the Task Force also recognizes that this information must not be removed from polling places, if the law is to achieve its dual purpose of protecting voter information and to encourage participation.

The Task Force considered extensively various options before arriving at the following recommendation:

- The Secretary of State should seek to amend the Elections Code to require that a notice be posted in conjunction with, or on the voter roster, or otherwise prominently displayed at polling places that informs the public that theft or removal of the voter roster from the polling place is a crime.

The Task Force did not agree unanimously on the above Recommendation:

Task Force Members Linda Berger and Beth Givens opposed Recommendation Number 10, while the remaining five Members of the Task Force voted to adopt the Recommendation. Task Force Members Givens' and Berger's reason for opposing Recommendation Number 10 is provided below.

Linda Berger and Beth Givens Statement of Opposition to Recommendation Number 10:

"We believe the Task Force's Recommendation does not go far enough. Current practice, required by law, is to publicly post the names and addresses of everyone registered to vote at that

particular polling place. The Task Force learned that these listings are sometimes stolen. The Recommendation favored by the Task Force is to post a sign next to the list telling individuals that it is a crime to remove the list. We recommend instead that only the individual's name be posted and that addresses and other information such as phone numbers be excluded. In the 12 years that the Privacy Rights Clearinghouse has existed, many individuals have contacted us to complain that their names and addresses are posted at the poll. They feel it is a violation of their privacy for anyone to be able to see this information."