Minutes:

Task Force on Voter Privacy
November 5, 2003
10 a.m. – 1 p.m.
Sacramento, CA

Members present: Chairman Willie Pelote; Members: Dave Wong; Jim Hayes; Linda Berger; Victor Salazar; Beth Givens; Bill Cavala

Mark Kyle, Undersecretary of State, began the proceedings by thanking Task Force members for their service on behalf of the Secretary whose attendance was delayed; the Undersecretary then swore in the Task Force members.

Chairman Pelote began the meeting by recognizing the Undersecretary for opening remarks.

Undersecretary Mark Kyle explained the interest of the Secretary in privacy and participation in democracy, including his authorship of legislation (AB 2832, Ch. 959, Stats. 2002) requiring the creation of the Task Force. The prohibited commercial use of the voter file information, the potential for identity theft and the potential for altering the outcome of elections were primary concerns for the Secretary. But there is a need to balance privacy protection with the openness of democracy. The Task Force's charge is to balance these interests, to examine existing laws and to determine the adequacy of existing safeguards.

Chairman Pelote citing AB 2832 informed the Task Force members and the public of its potential responsibility to recommend adoption of uniform guidelines and legislation for introduction as a result of the proceedings. He mentioned the "aggressive agenda" of the Task Force and outlined future hearings. The Chairman outlined the rules of conduct for the hearing and commented that equal weight will be given to Task Force and public comment during deliberations.

The Chairman introduced the panelists for the hearing—Secretary of State Elections Division Chief John Mott-Smith and California Voter Foundation (CVF) Founder and President Kim Alexander.

Panelist #1—Kim Alexander (CVF)

Kim Alexander identified the California Voter Foundation as a decade-old, nonprofit organization. She said that California had pioneered the use of the Internet for campaign disclosure, and complimented the Task Force for being the first of its kind in the nation. Being on the "cutting edge" of technology creates risks. Voter profiling and targeting by campaigns, coupled with the availability of data was noted. The federal Help America Vote Act of 2002 (HAVA) requirement for collection of personal data (driver's license number or partial social security number) and the mandate to create a single statewide voter file created additional risks.

CVF conducted a study of state laws and practices regarding—what information was collected; what notice is provided to voters re: data collected; what unique data is collected by states; what data is redacted or withheld when data is provided to secondary users (users who are not election officials); and what use is allowed by secondary users.

Data Collected by States

- All states collect names, dates and signatures.
- All states also collect date of birth.
- Phone numbers are collected by 46 states—18 require it; for 28 it's optional…some state require both a home and work number.
- Gender information is requested in 34 states.
- Social Security numbers are requested in 9 states.
- Party affiliation is requested in 29 (all allow a decline to state option).

- U.S. citizenship affirmation is requested in 18 states (HAVA will make this a national standard).
- Place of birth is required by 14 states.
- Race is noted in 9 states (for six it is optional).
- Drivers' license numbers are requested by 11 states.
- Various states request voter information about poll worker interest; voter needs for special assistance; parents' names; e-mail addresses (2, one of which is California); and occupation.

Notice to voters

- All states notify voters about a penalty for providing false information (California is unique in notification about a prohibition on commercial use of data).
- Two-thirds of the states requesting Soc. Security number provide voters with explanation for requesting
- For optional and mandated information—38 states inform voters of optional fields; 11 provide no notice
- Public Notice—four states provide notice to voters that the information is a public record or accessible
- Only 1 state (Iowa) make voters aware of secondary users

Lack of notice about secondary use and optional fields does not allow voters to make an informed decision about registration
Giving up too much data on voters to secondary users might deter registration and further depress turnout

States that redact (withhold) information provided to secondary users

- 11 states withhold the Date of Birth information in some fashion (partial or total)
- 5 redact phone numbers
- None withhold the gender information
- Two do not provide birthplace
- Driver's license information is kept confidential in 6 states
- None of the states withhold race/ethnicity information

(Note: These "actual numbers" must be placed in context of the number of states collecting the data—which is not available to me right now.)

States that suppress access to records

- 24 states do not offer this option
- Those states that do offer this option to voters usually restrict the option to public safety personnel, stalking victims, victims of domestic violence

Purpose of use of data by secondary users

The general categories for allowable secondary users are:

- Political/campaign purposes
- Nonprofits
- Government
- Academic
- Commercial (California does NOT allow commercial use)
- Journalistic

Typical secondary uses:

Political/campaigns—used to send mailers and to contact voters; there is the ability to add "value" to the voter data by merging with other databases (e.g. magazine subscriptions); this information can be used to target voters (e.g. Democratic voter/Latino surname/no Republicans in the household)…this information can now be produced in hours, instead of days..

Campaigns are able to target likely supporters, but other voters are ignored—this may be contributing to a decline in turnout

Jury duty—34 states use voter lists—national survey indicates that when voters are aware of this, it deters them from registering to vote

Incumbent use (in Califomia)—In California, incumbents use the voter file to target mailings to constituents…in the summer of 2002, 7 million mailers were sent by sitting legislators at a taxpayer cost of $3.5 million…one member targeted 47,000 women with a mailing…another targeted 35,000 seniors…so there is targeting for not just voters (by campaigns), but constituents (by politicians)…this is exclusionary

Scholarly—usually to study trends in voting, voting turnout generally and by specific demographics

Journalistic—this may be used as a way to find a source (address, phone number)—4 states expressly provide access. Newspapers are commercial enterprises (selling newspapers), but this is balanced by the First Amendment status and rights provided to news outlets.

Commercial use—22 states are collecting more information than is necessary for strictly election purposes and distributing the information for commercial use without notice to the voters (California prohibits commercial use of this data).

Recommendations (for California):

- Add voter notice—improve security, review what is provided and requested now
- Clear instructions re: optional fields (what's really required)
- Limit data collection—are optional fields really necessary
- Restrict secondary distribution of sensitive data—date of birth, place of birth, et. al.
- Database security—in May 2002, the State Controller's database was hacked providing access to records of 260,000 state employees
- Internet voter registration—creates potential for unwanted access
- Commercial use—strengthen the parameters of the prohibition on commercial use

Use the (four) principles of the Federal Trade Commission to guide Task Force discussions:

- 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 get access to the data
- Access—voters should be able to request from government an accounting of data government has on file
- Security—assurances that the data is protected

Voting is a sacred right of democracy…we must protect it.

Panelist #2—John Mott-Smith (Secretary of State Elections Division Chief)

John Mott-Smith offered the perspective that voter privacy is a microcosm of larger issues being debated especially after September 11, 2001. Voter records are neither completely confidential nor completely open. There are other analogies as well—California has neither a closed primary, nor an open primary, but

a “slightly ajar” primary that allows voters not affiliated with a political party to participate in the “closed” nomination process of parties conducted in primary elections.

There is a general principle that government is open for good and valid reasons—where a candidate lives, and what voter registration records show are important to establish eligibility for both and this protects the integrity of the process. But there is also an increasing desire and need to keep information confidential.

A sample of the voter registration affidavit used to suppress certain voter information for peace officers was provided as an example. In addition, California has—prohibited disclosure of the list of voters requesting minority language voting materials; kept confidential the registration of certain other persons (celebrities, stalking victims, domestic violence victims), all of whom become absentee voters. California also now has a process to seek a court order to keep voter information confidential at the request of any voter on a case-by-case basis.

There is not a single voter registration form used in California. There are 85 forms. With 58 counties, some of which customize their affidavits and six languages required for minority language voters, there are multiple forms. There are also millions of forms that meet federal Motor Voter (National Voter Registration Act of 1993) requirements provided to the Department of Motor Vehicles annually, as well as social service agencies.

Effective January 1, there is a law to distribute voter registration forms in 3 million Tax Booklets mailed by the Franchise Tax Board to taxpayers’ homes.

Certain information is required on all forms—name, address, date of birth, but even these are not without controversy. Former Secretary of State March Fong Eu refused to provide the year of her birth on the affidavit. When other voters followed this practice it created a problem for a secondary user—the federal Selective Services, which requires registration for the military draft when citizens turn 18. Selective Services used the voter file and ended up sending draft board notices to people in the 80s and 90s.

Signatures of voters are always required—it establishes identity for use in absentee and provisional balloting, for instance.

Next year, California will be required to request voters to list their ethnicity on voter registration forms.

HAVA will now require the last four digits of a voter’s Soc. Security number or a driver’s license number, which is currently optional in California, which must be entered into a statewide voter registration database and verified against either the Soc. Security database or the DMV database.

There are potential advantages of the new federal requirement for a statewide voter registration file—including the future potential to allow voters to vote “from anywhere” (with access to the database and access to the appropriate ballot style).

Voter registration forms will also change under the federal law—it must ask if a person is 18 or if they are a U.S. Citizen.

The telephone is a desired field on the affidavit because it can be used by elections officials to resolve voter issues—incomplete cards, questions about absentee ballots. The e-mail address that is also an optional field may not be working as intended—there is less use by elections officials.

Signatures are a vital part of the affidavit, and a new law will allow the Secretary of State to collect digitized (electronic images of manual signatures) gathered by the DMV when it issues a driver’s license. With a statewide voter file, this will help update voter records that “cross” county lines.

The breadth of the exceptions (political, scholarly, journalistic) to the generally confidential status of voter records is considerable. The journalistic request is limited to those that can demonstrate credentials, but it

is potentially large—e.g. a writer whose work will be published in installments in a magazine or newspaper may request access to the voter file, but the response is not clear cut.

Political and scholarly uses are similarly broad terms.

Regulations provide that commercial use is prohibited. Violations carry a 50-cent per signature fine. There does not appear to be a demonstrated problem at this time.

Jury duty is an example of a legitimate governmental use, but studies indicate that 4 percent of the population does not register to vote because they do not want to be called for jury duty.

There are also scenarios that could potentially create confusion:

Commercial use is forbidden, but could a Wal-Mart use the voter file to contact voters to lobby the city council on a zoning change to build a store—this is both a political and commercial use, but which prevails. If voters want the file to collect signatures for a petition drive to stop a Wal-Mart from being located in their area that seems a legitimate use, but if the first example results in a restriction, what is the rationale for a decision in this case?

Problems arise with the voter file, and there is a concern about voter privacy, misuse of information and commercial use, when unscrupulous "bounty hunters" who are paid on a per signature basis to collect petition signatures or register voters get involved. Documents are falsified some times, party affiliations are changed, or signatures are grafted onto petitions the voter never signed I some cases.

"Skip tracers," those who are hunting for "bail jumpers" consistently request voter registration file information, but without a court order, this is not seen as a legitimate government use of data.

There is also a concern about the definition of commercial use itself—if a single data point is extracted (e.g. date of birth) from the voter file and used to augment another database is this an improper use of the "voter file."

The biggest complaint the Secretary of State receives about "inappropriate" use of the voter file is about unsolicited contact by campaigns, especially "negative" campaign pieces.

There are occasionally issues with political consultants who request access to the voter file before they have a client for the data. The legitimacy of the political community is recognized, but to protect the legitimate use of the list a standard must be maintained and a chain of custody must be established for enforcement purposes.

Recommendations

In the many years during which this issue has been dis cussed, there is no clear answer about where to draw the line or how to provide the balance. There are some additional suggestions from a program standpoint:

- Allow for "salting or seeding" the file with fictitious names—if that name is used in a commercial mailing, the improper use of the voter file could be established and the person responsible could be traced.

- Provide explicit authority for penalties—the penalties are regulatory now and with no administrative remedy, the authority to fine a person for a violation might be challenged.

- Simplify the voter registration form—the act of simplifying the form to make it more user friendly might also raise the question about what personal information is necessary for election purposes.

TASK FORCE QUESTIONS, ANSWERS AND COMMENTS:

TF member Beth Givens asked whether salting or seeding the voter file was prohibited and whether legislation was needed to provide the authority to do so.

John Mott-Smith said it was "an open question," but that explicit legislative authority would be helpful.

Kim Alexander said that other states do salt their voter files and it addresses the issue of uncovering merges of lists.

TF member Givens reported that the DMV performs audits to determine if there is misuse of its data files by employees or secondary users. Does the Secretary of State perform audits?

John Mott-Smith responded that there were no resources to perform audits, but that specific complaints could be and are investigated.

TF member Victor Salazar commented that the Secretary of State is not the only source of voter file information; all 58 counties maintain a voter file of voters in their jurisdiction.

Kim Alexander did request the statewide voter file, and showed the Task Force members the letter that accompanied the file (on CD ROM) explicitly prohibiting the distribution of the list to other users without permission.

TF member Bill Cavala provided those in attendance with a short sketch of his background (university professor, overseeing election activities statewide, and direct involvement in a handful of elections each cycle). He raised the question of balancing the privacy of the voter, the rights of campaigns to data and the impact on democracy (voter information and participation).

Kim Alexander responded that the key phrase, she believes, is "informed consent." Those in the political world understand that there are secondary users of the data. But the public becomes angry when someone arrives at their doorstep with personal information about them and others in their household. There should be more disclosure that there is access to the data…more information about what data is optional for the voter to provide…and/or consent about use of the data (e.g. yes allow election official use, but no to campaign use).

TF member Cavala commented that voter files were initially used to restrict access to the polls (through voter eligibility standards) and to look for voter fraud (of which less than a handful of examples have been found), so the use of the data has become largely political, but the check on excesses is the angry voter—a person who is alienated, won't listen, or creates a backlash.

Kim Alexander reiterated her concern that selective targeting ignores some voters and may depress turnout.

Secretary of State Kevin Shelley was recognized by the Chair. The Secretary thanked the members for their service. Creating the Task Force was not the central purpose of the legislation when he engaged the issue; he was primarily concerned about ensuring strong safeguards against commercial use of voter file data and more certain enforcement of violations. But there is a convergence of issues that has highlighted the need for information security and has expanded the mandate of the Task Force. He looks forward to its recommendations.

TF member Cavala related his personal experience with focus groups interviewed about attitudes about voting and voting behavior. The focus group members then discovered that researchers had actual records of their voting history (how often, not how). The focus group members seemed embarrassed when

confronted by their voting history. He commented that the conclusion could be drawn that "shame"—produced by public disclosure of voting history—seemed to be a powerful motivator for voter turnout.

Kim Alexander commented that polling place rosters, which are posted at each polling place, keep a running tally of who has voted; on a small scale, this was public disclosure of voter history. She also said that putting the information online had been suggested, but that it was a radical idea she did not recommend. In response to a question from TF member Cavala, she said she was unsure what effect such disclosure would have on voter turnout.

TF member Cavala commented that he believes public disclosure of voter history would depress voter turnout.

TF member Cavala went on to discuss anecdotally the impact of the political use of voter registration data—voters who received 24 pieces of political mail from one particular candidate over the four days preceding Election Day. When the same voter was contacted to inquire about his attitude toward the candidate, the voter said, "he thought he had heard of the candidate."

John Mott-Smith reiterated that the issue is not clear cut—a balance was needed. He urged the Task Force to consider the need for simplicity of the process. If elections officials were required to categorize voters according to their stated preference about who could receive voter file information (e.g. elections officials, but not campaigns…journalists but not scholars), the process would become unwieldy. He said he could not quantify the number of voters who requested to be removed from the voter rolls because of negative reaction to contact from campaigns, and that people may well still participate even though they complain.

TF member Cavala commented that one landmark study indicated that reaching voters with information and "hoopla" around campaigns is a better indicator of voter participation even than voter agreement with a candidate on issues. He also said that campaigns are akin to small businesses and lack the resources to create sophisticated, cross-referenced and merged databases of the sort described by some.

Kim Alexander commented that one particular vendor contains the voter file, voter ethnicity, magazine subscription and charitable contribution (including political contribution) data. She also said a student astonished a college professor by purchasing personal information about the professor from a database company for $25.

TF member Cavala reiterated the limit on campaign resources, which would make a $25 per record database cost prohibitive.

TF member Givens asked about the four states providing notice to voters about public disclosure.

Kim Alexander said New Mexico, Tennessee, Texas and Iowa provided notice that voter file information was public and Iowa provided the most thorough notice to voters.

TF member Victor Salazar requested copies of the letters that accompany disclosure of statewide voter file data. He also asked what occurs when a District Attorney, the Attorney General or the DMV requested information.

John Mott-Smith said a legitimate governmental request results in automatic access to the voter file, including requests from all levels of government agencies (local, state and federal).

Chairman Pelote asked whether the request had to be accompanied by an explanation and criteria for the use of the data.

John Mott-Smith said yes, and clarified that there are occasional and regular users of data—regular users are allowed to apply once and provide the explanation of the use of data and then receive the data regularly without making separate application.

TF member Dave Wong asked if there was any study that suggested one form of complaint—campaign contact by mail or phone—or from a particular area—one or more counties—was more prevalent?

John Mott-Smith said the data did not exist; Kim Alexander said that the Secretary of State receives the most complaints, but no analysis or data was available.

TF member Linda Berger expressed her view about the need to balance the interests involved, expressed an interest in receiving specific recommendations from panelists for California, and was interested in a county perspective on the issue. She also asked further about the disclosure provisions in California law.

Kim Alexander said that California gets mixed reviews re: disclosure. Commercial use is prohibited and it is the first state to specifically state on voter registration affidavits that commercial use of the voter information is a misdemeanor. There are four optional fields on the affidavit, but the language used to convey that fact may be confusing—failure to provide the information is not the basis for denying registration—the language uses a triple negative. Voters would be better served by having the instructions for filling out the affidavit at the top of the form, so they know the rules before filling out the affidavit. Optional fields should be more obvious. Providing the e-mail address made regulation difficult because it raises First Amendment issues, but voters would probably react negatively to political "spam." The election official use is questionable, e-mail can more readily be seen as a secondary use.

TF member Berger commented that in the absence of voter fraud evidence, there was a need to seriously consider what information was absolutely necessary. Reducing the concerns about registering to vote, especially for those concerned about stalking or domestic violence, needed to be a concern for the Task Force.

Kim Alexander noted that the only statewide public awareness ad for the Safe at Home program (which allows victims of domestic violence, stalking victims and reproductive health care workers in some cases to keep address information confidential) that she was aware of was in the state's (voter) ballot pamphlet. Those at risk would not register to vote, and so would not receive a pamphlet. Public awareness campaigns targeting these groups were important so that they realize they can register to vote while maintaining confidentiality.

Chairman Pelote asked about the similarities of voter registration affidavits statewide.

John Mott-Smith noted that "99 percent" of the information requested on the affidavit is identical statewide, but that there are differences.

TF member Salazar also posed the question about access to absentee ballot application information. (Campaigns often send mailers to voters that include an absentee ballot application that is mailed back to the campaign for forwarding to election officials.)

Kim Alexander recommended that the "universal" voter registration affidavit should serve as the baseline for determining what information should be included in the voter registration affidavit.

TF member Salazar asked the Government Code said about voter confidentiality. (Note: See Govt. Code Section 6254.4 provided in the TF member binder.)

TF member Cavala commented about the difficulties of restricting and defining secondary users. Campaigns are an integral part of achieving voter outreach, education and turnout—they are clearly a secondary user. Should there be a restriction on governmental users—district attorneys, jury commissioners, etc. Journalistic purposes defy descriptions…journalists consider themselves "the public," but accept the designation in order to do their job and for First Amendment protections, but what, for instance, defines a "newspaper." Commercial use has not been adjudicated to an extent that provides any guidance.

TF member Givens asked whether it was possible to get a case study of the list of names provided to a campaign that included social security numbers.

TF member Jim Hayes said that in his experience no with social security numbers is available. He speculated that a union membership list being used by a campaign would likely contain social security list, but that lists that are publicly and commercially available do contain that information.

TF members asked about the new federal requirements for providing driver's license and Soc. Security numbers.

Kim Alexander commented that it had potential to "be a logistical nightmare." DMV's track record on Motor Voter has been poor. In response to a question from Chairman Pelote, she added that HAVA was intended to address "Florida" election issues, but that it became a potpourri of election law changes.

TF member Givens asked whether there was a list of HAVA concerns written down that the Task Force could have for the record.

TF member Salazar commented that there is not just one point of access to voter file information, but 59 (58 counties and the Secretary of State).

Kim Alexander said the "bright side" of HAVA was that a centralized data meant there was one focal point, one set of rules and procedures for information, one key enforcement entity. She also said that it appeared as though producing voter files was a frequent request of counties—L.A. County, for instance, featured information about requesting the voter file prominently on its website and in its offices. Counties might resist statewide restrictions, if it was a revenue generator in these tough budget times.

John Mott-Smith pointed out that the cost of producing the voter file is restricted to the actual cost of producing the list, so it could not really be a revenue source.

TF member Salazar also commented that centralizing all requests for the voter file would be a huge burden for a single agency. And some requests are for only a portion of a county file.

TF member Cavala "for the record" publicly stated that a driver's license number and a Soc. Security number are of no value to a campaign; similarly, any unique identifier required under HAVA would be of no value; a unique identifier would be of value to elections officials to help identify duplicate registration where the voter had re-registered but used a variation of their name (e.g. Bill instead of William…the addition of a middle initial…etc.). Soc. Security numbers are particularly sensitive as unique identifiers, he added, because that is where fraud and identity theft can occur.

Kim Alexander commented that once data is created there is a reluctance to alter it or surrender a part of it because the list is valuable. A centralized database would help ensure that the appropriate information is redacted from lists, but that she was concerned about the dissemination of the voter file to other state agencies out of concern that the procedures for withholding information would be diluted at other agencies.

TF member Cavala made Task Force members aware of a state Constitutional Amendment pending on the Assembly floor that had the potential to obliterate privacy protections with the a Constitutional right to openness and access.

Chairman Pelote asked for public comment and further Task Force comment. There was none.

The Chairman announced the next hearing—November 12, 2003; San Diego County Administration Bldg., 1600 Pacific Coast Hwy., Rm 358, San Diego, CA from 10 a.m. to 1 p.m.

The Chairman adjourned the Task Force at 1 p.m.