Minutes:

Task Force on Voter Privacy
November 21, 2003
10 a.m. – 1 p.m.
San Francisco, CA

Members present: Acting Chairman Victor Salazar; Members: Dave Wong; Linda Berger; Beth Givens; Bill Cavala.

Acting Chairman Victor Salazar began proceedings at 10:00 a.m. He gave his opening remarks and introduced Tom Newton. The other two panelists were not present at the start of the hearing.

Panel #1 – Should Certain Voter Records Be Confidential
Panelist - Tom Newton, California Newspaper Publishers Association
Panelist - Kathleen Krenek, Next Door, Solutions for Domestic Violence
Panelist – Tim Fries, Governmental Affairs, CA Union of Safety Employees

Tom Newton representing the California Newspaper Publishers' Association (CNPA) provided the Task Force members with an overview of the privacy issue from a journalist's perspective. 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); to evaluate redistricting proposals by the legislature and others; or to establish a subject's or source's "identity" (are they who they claim to be). He said that misuse of public records is a crime. The CNPA advocates for public policy that denies access in the case of demonstrated "bad acts," but argues that policies must weigh toward public access unless public interest in denying access clear outweighs the interest in granting public access.

Task Force member Beth Givens commented that she considered journalistic access crucial. She asked, without any established licensing for journalists or other objective credential, whether Mr. Newton would suggest any definition for the term journalist to help clarify when access should be limited.

Mr. Newton suggested that a definition would be very difficult to achieve. The First Amendment (granting freedom of the press) 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 possible, so a signature and affidavit must be sufficient.

TF member Givens agreed that the press should not be licensed in a legitimate democracy, but it still leaves the concern that a stalker or other person with malicious intent might claim to be a journalist.

TF member Bill Cavala asked whether a more rigorous definition of journalistic "purpose" (as opposed to a definition of journalist). Could we list those uses and make other uses, or misuse, a crime? He also commented on the ban on commercial use, while pointing out that journalistic uses ultimately support commercial enterprises.

Mr. Newton commented that the commercial use restriction is relatively new. He told the TF that people were often surprised at the separation between the editorial and commercial side of the newspaper business. As a representative for newspaper publishers, he sometimes approaches members of the Legislature who ask him why he is advocating a position, when a newspaper among his "clientele" has written an editorial that is contrary to his position.

TF member Cavala commented that the exemption for political campaigns are in part because elected officials are public officials, although candidates for office are not per se. Yet we require disclosure of financial interests and personal information as a prerequisite to running for office. Voters also are engaging in a public activity; one reason that the information is available is because people may engage in efforts to restrict voting. There is a balance, however. Is it a public act or a private personal act?

Mr. Newton said jury service presents an analogous situation. People cannot opt out of jury service, however. 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 polling booth is drawn.

Chairman Salazar recognized the next witness—Kathleen Krenek the Executive Director of Next Door, Solutions to Domestic Violence. Ms. Krenek said she had 30 years of experience in the domestic violence victim advocacy arena and currently operates a full service shelter and assistance program in San Jose that has more than 11,000 contacts a year, helping victims to obtain restraining orders, provides teen battery and intervention programs, and provides transitional living facilities to victims of abuse. She provided the TF with a review of her extensive resume. Battered women's advocates often contest the "public interest" doctrine on open records because they advocate for the rights of victims to personal safety. The Safe@Home program is used extensively now by her organization, and more than ever before address confidentiality helps victims—to live in the same city, county, state or even another state in safety. Ms. Krenek told the TF that batterers can be 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. 80% of women are victimized after they leave or consider leaving an abusive relationship. Whole families can end up dead if they are "discovered" by an abuser. The very practical reality is that only 4-10% of victims enter protective programs. Early concerns that the program would be used as a means to evade bill collectors, or for other inappropriate uses, has not materialized. On

the other hand, personal stories provide examples of what must be surrendered by victims of abuse to escape violence—giving up educational degrees, family associations, community life, even religious affiliations. 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. Legal minds can work on this issue to find solutions.

TF member Cavala said that operating under the existing exemptions granted to the four secondary users (journalists, scholars, political parties and campaigns, and governmental users), voter registration records might be accessible. Does she discourage her clients not to register to vote?

Ms. Krenek responded that it was a very difficult issue for her—she is a strong believer in civic participation. She said the TF would have to balance the right of access to the right of privacy to allow for that civic participation, if possible.

TF member Linda Berger asked whether the Safe@Home program offered protection. She said her impression was that the program provided that protection, but that it was inadequately funded—including outreach and education efforts to build public awareness about the program's existence.

Ms. Krenek agreed that the Safe@Home program was the answer, but that more awareness was needed.

Chairman Salazar asked the Secretary of State staff to provide the TF with more information on the Safe@Home program.

TF member Dave Wong asked Ms. Krenek if she had ever surveyed her clients to determine whether they still vote.

Ms. Krenek said she had not.

TF member Wong asked if batterers find women she is helping escape abusers.

Ms. Krenek said yes, if you want to know where the domestic violence shelter is located, ask a batterer. Police help shelters make sure that batterers do not abuse shelter residents. Domestic violence is generally perpetrated in private, and abusers are less likely to commit acts of abuse openly—at a shelter. She did offer an anecdote about an abuser who sent a tiara and roses to a victim at the shelter address, and responded with a picture of a tombstone with the victim's name written on it, when she did not respond positively to him.

Chairman Salazar recognized the next panelist Timothy Fries, representing the California Union of Safety Employees—law enforcement personnel.

Mr. Fries related an anecdote of a code enforcement officer from the Department of Food & Agriculture who had to exterminate ducks and chickens that had contracted New Castle's disease. The animals were family pets. The 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." Mr. Fries said the TF must perform a balancing act—removing all peace officers from the voter rolls would mean a loss of several hundred thousand records. However, the ability to access the voter rolls with a promise that "I am not a liar" did not seem adequate. Mr. Fries suggested that notification to persons whose records had been requested, or a higher standard than a self-avowed "I am who I say I am" to access the records was appropriate.

Chairman Salazar commented that state law does allow restriction to individual records via a court order with good cause.

TF member Cavala said that a mail drop (Safe@Home is a mail forwarding and address confidentiality program) for peace officers or domestic violence victims still enables people to contact the individuals, but if the mailing handling service eliminates "junk mail," it might eliminate the effectiveness of political communications.

TF member Cavala posed the question: Could a vendor ask for the list of Safe@Home enrollees, under the exceptions granted for access to the voter registration list, and receive the list? If so, how is the list maintained—are those with confidential records "flagged" according to the reason for the exemption (e.g. peace officer).

Staff said they would survey counties and seek legal counsel's interpretation on the question.

Chairman Salazar requested that a meeting of the TF following the final December 15 hearing, so that members could discuss the proceedings and formulate final recommendations.

TF member Givens also related an anecdote about the inadvertent distribution of confidential information when competing local telephone companies shared customer files to create a single telephone book. In California, where 50% of customers ask for private numbers, one company provided this data and it was printed in the public phone directory. This incident and its aftermath showed that privacy is an important issue not just for stalking victims or domestic violence victims.

The TF took a short break.

Panel # 2 – Enforcement of Privacy Laws & Status Report
Panelist – Susan Oie, Deputy Attorney General, CA Department of Justice
Panelist – Ric Ciaramella, Chief Investigator, Election Investigation Fraud Unit

Chairman Salazar introduced the next panelist—Deputy Attorney General Susan Oie. Ms. Oie provided the panel with an overview of the status of commercial access to public records. A commercial vendor had asked for access to arrest records and was denied the data by the Los Angeles Police Department. The U.S. Ninth Circuit Court of Appeal had ruled that the records were confidential. But the U.S. Supreme Court ruled otherwise on a different case. In reaction to that ruling, and with respect to voter registration information, a challenge to the confidentiality of those records was initiated. Ms. Oie said that in preparation for the case, she took a deposition from Professor Price from the Annenberg School of Journalism at USC to distinguish between commercial use of the data and journalistic use. Journalists use this data as a public watchdog for voter fraud; to assist the public in making intelligent electoral decisions; to validate campaign information (e.g. candidate eligibility); for polling and research verification. She cited Justice Potter Stewart's comment about the need for a fourth check on the three branches of government to ensure the integrity of the process.

She distinguished the journalistic use—for specific purposes—with the commercial use—no stated end use for the data, other than to sell it to a user whose purpose was undefined. The commercial vendor lost the case. In addition to laws already discussed, the Information Practices Act of 1977 articulated standards and reasons for keeping the data private, and these sections of law explicitly supersede the Public Records Act provisions. 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. The Attorney General would defend that nondisclosure, and it is highly unlikely a judge would rule contrary to that position—the public interest in nondisclosure is outweighed by the public interest in disclosure in those cases.

Chairman Salazar asked whether Ms. Oie's experience provided any definition of journalist that could be used for purposes of the law.

Ms. Oie said no definition was available that she was aware of—only the deposition from Professor Price that described the uses of the data.

TF member Cavala asked if the Safe@Home list would be available under the exceptions.

Ms. Oie said no Elections Code Section 2194 would apply; the confidentiality exists independent of the four exceptions that apply generally to the voter registration file with names that had not been granted confidentiality under other sections of law.

TF member Cavala asked whether that was the position of the Attorney General.

Mr. Oie responded that the Attorney General did not have a position on the question; it had not been posed to the Department.

TF member Cavala asked whether her impressions would hold true if SCA1 (a constitutional amendment pending on the floor of the Assembly) became law.

Ms. Oie cited sections of SCA 1 that state it does not supersede other privacy protection granted under other statutes.

TF member Givens asked whether any TF members were aware of whether any apparent conflict between SCA 1 and existing privacy statutes would be tested in the courts.

TF member Cavala said that discussion among legislative staff and attorneys indicated that the intent of SCA 1 was to limit the effectiveness of existing privacy statutes and to give access to records a constitutional weight on a par with the right of privacy in the state constitution.

TF member Givens asked whether a voter registration affidavit was a state or local record and whether the Information Practices Act extended to local records.

Secretary of State staff said they would seek legal clarification on this question.

Chairman Salazar introduced the next panelist, Ric Ciaramella, the lead investigator in the Secretary of State's investigative unit.

Mr. Ciaramella sought to clarify a comment at an earlier TF hearing in which it was related that petition signature gathering fraud was not investigated—the Secretary of State's office does investigate and has helped secure 44 convictions that resulted in cumulative sentences of 15 years in state prison, community service, etc.

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, but no case has been prosecuted under the statute. Cases involving commercial use and sale of the information over the Internet were pursued as a criminal matter, but adjudicated as a civil matter. 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 in this arena stem in part from the broad definitions that adhere to the exceptions. A person who questioned investigators about how to request the voter information file because he was a "free lance" writer turned out to be legitimate—the piece he was writing ran in the L.A. Times.

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 a registered sex offender. It is common that bounty hunters have a criminal past—90% of them have a record.

Chairman Salazar asked if the 90% figure applied to the entire database of 1,000 bounty hunters, or just those convicted.

Mr. Ciaramella said it was the entire database.

Mr. Ciaramella suggested that the TF could consider using the DMV model for voter confidentiality—a simple request by the voter to keep their record confidential. In five years, the issue will become even bigger because of the growing sophistication of the Internet. He suggested that the TF consider looking at models for privacy being considered by other agencies—including the Department of Justice. Judge James Brown heading up a panel for public safety issues.

TF member Berger asked whether Mr. Ciaramella believes the penalties for violations should be increased.

Mr. Ciaramella commented that federal court decisions sided with bounty hunters rights to participate in the process. He said he would like to "get an audience" with the California District Attorneys Association to provide a better understanding to district attorneys about the law, and that he would like to create stiffer penalties. Laws that require paid signature gatherers to be reported to report to local registrars, show identification and fill out a form would be helpful.

TF member Cavala commented that there was a legislative proposal to require petition signature gatherers to be registered voters, but that it did not gain support from either party. Signature gathering is one of the few jobs available to ex-cons; "at the bottom of the scale." He commented, though, that the number violations seemed to be on the decline and asked for Mr. Ciaramella's comment.

Mr. Ciaramella responded that he did not have statistics available to show trends with him, but that 14 cases had been prosecuted this year, and that investigations typically take 18 months to conclude before a prosecution can be pursued. The sophistication of the practices that are subjects of complaints do seem to be on the rise.

TF member Cavala and Mr. Ciaramella discussed the relative impressions over non-citizen voter fraud, whether it was committed and by whom, and whether cases were investigated and whether there were any convictions at the state level. Mr. Ciaramella said there were referrals, but no convictions.

TF member Givens asked how commercial use might be discovered by the Secretary of State.

Mr. Ciaramella said that the Secretary of State "seeds" its list (adds fictitious names). Although the Secretary of State is typically among the first to hear of potential commercial use of the voter file, it is difficult to trace back.

Chairman Salazar asked for public comment. There was none.

Chairman Salazar announced that the next TF hearing will take place in Los Angeles at a location to be determined on December 15.

The meeting was adjourned.