International Outsourcing of Voter Information: Risks to Our Privacy?

Prepared by Counsels of the Assembly Judiciary Committee for the Committee's Special Voter Privacy Hearing on March 15, 2005[1]

What bank robbery was to the Depression era, identity theft is to the Information Age.

-- Sen. Charles E. Schumer (D-N.Y.), 2005.

PURPOSE AND SCOPE OF THE COMMITTEE'S REVIEW

This special hearing of the Assembly Judiciary Committee was called by the Speaker of the Assembly in response to alarming press reports, recounted below, that a California-based political action committee seeking to qualify proposed ballot initiatives reportedly may have outsourced or shared California petition signer and/or voter information with personnel in India in order to save money when verifying petition signatures. It is very important to note at the outset that the Committee's review of this matter has only just commenced. The Committee requested information from the parties reportedly involved, including any applicable contracts that may speak to confidentiality and privacy issues, and it is hopeful that this information will be produced following continuing efforts by the Committee to receive it.

Regardless of any contractual security promises made, however, this potentially unprecedented international outsourcing or sharing of voter or petition signer information abroad (which may even include unlisted home addresses and phone numbers, voting preferences and histories, as well as prior residence histories) clearly raises important privacy concerns of statewide and, therefore, legislative importance. The FBI has reported that many identity thefts that occur in the United States are hatched internationally. A leading bank regulator, the Federal Deposit Insurance Corporation, warned recently that increased outsourcing of jobs overseas has heightened the risk of identity theft.[2]

IDENTITY THEFT: WHY SHOULD WE CARE?

What is identity theft? There are numerous variations. Essentially, this crime occurs when someone uses bits and pieces of information about an individual to represent him or herself as that person for fraudulent purposes. Examples include obtaining credit cards and loans in someone else's name and then not paying the bills, opening utility accounts, renting an apartment, getting a cellular phone, and purchasing a car or a home. An even more serious type – criminal identity theft – occurs when the perpetrator uses the stolen identity to commit crimes in the victim's name, giving the victim a criminal record.

---

[1] This paper was written by Drew Liebert, Kevin Baker, and Elizabeth Linton, staff counsels to the Assembly Committee Judiciary Committee. They may be contacted at the Committee's offices with inquiries about source materials. Thomas Clark and Dana Mitchell are also thanked for their able assistance with this paper.

[2] O'Brien, Timothy, "Inside Local Business Identity Theft Defies Control," Palm Beach Post, Nov. 1, 2004.

Victims generally are not liable for the bills accumulated by the imposters, under state and federal law. But they do have the anxiety and frustration of spending months, even years, regaining their financial health and restoring their good credit history.

Identity theft is said to be the fastest growing crime in America. Last year nearly 10 million people across the nation were victimized, resulting in losses to businesses and consumers of more than $50 billion. California has the unflattering distinction of being the only state last year with more than one million identity theft victims. One in ten of the victims of identity theft have been Californians, and the state has five of the nation's top fifteen regions for identity theft, according to the Federal Trade Commission.[3]

It is therefore not surprising that recent opinion polls reveal Californians place protecting their right to privacy as a major concern. Identity theft is not a partisan issue; persons across the political spectrum share growing concerns that the cost of losing one's personal identity and privacy is much greater than an issue of dollars and cents. As this Committee has frequently heard from witnesses, victims of identity theft tell horror stories of the hundreds of painful hours they must spend talking to credit card companies, banks, insurance companies, and law enforcement officials and merchants just to clear their name and their credit.

The crisis has created sufficient concern that it recently led to the state's first identity theft conference, held just days ago on March 1, 2005. The conference partners included Governor Arnold Schwarzenneger, law enforcement officials, politicians, businesses, consumer advocates, and identity theft victims. All of the participants recognized that the state needs to do much more to protect the identity of California's citizens.

Identity theft concerns are inextricably intertwined with privacy interests. California has one of the strongest constitutional privacy protections in the world: its Constitution specifically

---

[3] Just some of the most recent notable example cases of personal information theft in California include the following:

- LexisNexis: On March 9, 2005 information broker LexisNexis announced that passwords and other personal information of 32,000 U.S. citizens from the company's data base had fallen into the hands of identity thieves. The FBI and Secret Service are currently investigating the breach.
- ChoicePoint: In February of 2005, ChoicePoint announced that it has electronically delivered names, addresses, Social Security numbers, financial information, and other details to unauthorized persons in the Los Angeles area regarding 145,000 persons – 35,000 of whom were in California.
- University of California, San Diego: In January of 2005, UC San Diego announced that hackers had gained access to more than 4,800 files of student's personal information in November of 2004.
- University of California, Berkeley: In March of 2004, the social security numbers of more than 2,000 UC Berkeley applicants may have been seen by other students due to a problem with the UC Berkeley website.
- H&R Block: In March of 2004, 50,000 Sacramento-area H&R Block customers received notice that a company computer containing their social security numbers and tax return information had been stolen.
- California Employment Development Department (EDD): In February of 2004, the EDD notified 90,600 persons that personal information, including social security information, may have been compromised when a hacker accessed a state computer server in January of 2004.
- In October of 2003: The San Francisco Chronicle reported on a medical transcriptionist in Pakistan who had subcontracted with a Florida firm that had a contract with a Texas company that did business with the Medical Center at UC San Francisco. The woman claimed she was not being paid for her work and threatened to publicly release some of the information she possessed if she was not paid immediately.

guarantees to every citizen an inalienable right to privacy. (Cal. Con. Art. 1, Section 1.) The state also has some of the nation's most extensive privacy laws, recognizing that respecting individual privacy rights is an essential component to building and retaining public confidence in the marketplace. Indeed, California is the first state in the country to have an agency dedicated to promoting and protecting the privacy rights of consumers: the Office of Privacy Protection.

OUTSOURCING OF VOTER INFORMATION: AN IDENTITY THEFT "STARTER KIT" THAT MIGHT EVEN THREATEN OUR VOTING INSTITUTIONS?

As noted in the hearings the Committee has held on the issue of identity theft, many academic and advocacy groups have been increasingly previously concerned that the government and American companies are not adequately protecting private information sent overseas to countries like India and China. "Let's call it what it is: we're offshoring identities," Judith Collins, associate professor at Michigan State University and director of the school's Identity Theft Partnerships in Prevention, has noted.[4] Interestingly, much of the personal information that is stolen is not confiscated by hackers or dumpster divers, but rather by a few dishonest workers. Some organizations are now calling for complete bans on sending confidential information overseas to countries that do not offer and enforce privacy protections.[5]

The international outsourcing of voter registration or petition signer information raises these same concerns. As noted below, voters provide the government with significant information on their voter registration forms, including their date of birth, birth place, address, telephone number, language, gender, and much more. The information may truly amount to an "identity theft starter kit" when it gets in the wrong hands.[6] Unfortunately, as discussed more fully below, due to the limitations of American (let alone state) law outside of our national boundaries, when our personal information gets in the wrong hands overseas, we are left with very little recourse. While much has been written about California's increasingly strong privacy protections and remedies, it has also been noted that many foreign countries like India and China have limited or no analogous privacy protections to effectively protect Californians when their identities are stolen.

It is well understood that voter registration is the initial step in citizens' involvement in the democratic process. Only registered voters are permitted to vote in a democracy to safeguard the principle that elections are fair and only those entitled to vote do so. In addition, under the California Constitution's initiative requirements, only those proposed initiative measures that have the support of a large number of petition signers may properly qualify to be voted on by the state's electorate. It is therefore no exaggeration to suggest that if voters come to believe that by signing an initiative petition or registering to vote they may risk becoming victims of identity theft through the outsourcing of their identities abroad, they may not sign, and they may not vote. And these fundamental pillars of our democracy could consequently suffer.

THE POTENTIAL INTERNATIONAL OUTSOURCING OF CALIFORNIA VOTER OR PETITION SIGNER INFORMATION: WHAT HAS BEEN REPORTED THUS FAR?

[4] Chris Seper, "Outsourcing Brings Identity-theft Risk," Cleveland Plain Dealer, May 24, 2004.
[5] *Id.*
[6] Secretary of State's Task Force on Voter Privacy, Final Report, June 14, 2004, at 9.

As reported by David Lazarus of the San Francisco Chronicle on March 8, 2005, Citizens to Save California (CSC), a political committee working closely with the Governor to place his proposed constitutional amendments before the voters, is apparently relying on an offshore company to electronically verify signatures being gathered as part of that process.[7] CSC states it was formed recently to promote the Governor's initiative proposals.[8] The entity has been reportedly seeking to raise as much as $50 million for that effort.[9] It is co-chaired by Allan Zaremberg, president of the California Chamber of Commerce and Joel Fox, president of the Small Business Action Committee, a business lobbying group.[10]

According to press reports, CSC has reportedly hired two signature gathering firms – Arno Political Consultants and National Petition Management – and those firms have apparently contracted with a company in Oregon to verify the signatures. The Oregon company, TechSpeed, in turn, has reportedly acknowledged outsourcing this confidential voter information to India, where it does most of its work, in the Indian city of Pune. According to the Chronicle report, CSC is attempting to gather about 5 million signatures by the end of next month. TechSpeed reportedly outsources or shares petition signature verification to India because it is cheaper to use Indian labor. [11]

In a press release dated March 8, 2005, CSC sharply criticized the Legislature's impending review of CSC's reported international outsourcing of California voter information. CSC stated in its press release that it "has hired National Petition Management and Arno Political Consultants on a contract basis to accomplish the difficult task of gathering the signatures necessary to qualify the ballot initiatives that CSC has chosen to support." CSC further stated that "the methods used by these companies are common and the voter information is public and widely available." CSC further asserted that "this investigation is a waste of time and taxpayers dollars, and precisely the reason we need to reform California's government."[12] It is not yet known how many or which CSC petition signatures may have potentially been disclosed to, or shared with, Indian personnel, what other personal voter data, if any, may have been disclosed, or if TechSpeed has been engaged by other initiative campaign committees.

What Information Regarding Petition Signers or California Voters Was Reportedly Outsourced to, or At Least Shared With, India?

Initiative petitions contain the signers' names, signatures, street addresses, city and zip code.[13]

---

[7] David Lazarus, "Citizens To Save California Farms A Little Menial Work Out To India", S.F. Chronicle, March 8, 2005.
[8] http://www.citizenstosaveca.org/who.html (accessed March 10, 2005)
[9] Specifically, CSC supports two proposed initiatives measures currently being circulated for signatures that would affect the rights and benefits of certain public employees. One proposal would prohibit specified public pension plans; the other proposal relates to public school teacher tenure. In addition to these two initiatives, CSC has stated that it may also campaign in support of six or more additional initiatives currently on file with the Attorney General, including measures related to redistricting, state budgeting, education and public pensions.
[10] Other members of the board of directors include Jon Coupal, president of the Howard Jarvis Taxpayers Association; Bill Hauck, president of the California Business Roundtable; Larry McCarthy, president of the California Taxpayers' Association; Rex Hime, president and CEO of the California Business Properties Association; and Janet Lamkin, President and CEO, California Bankers Association.
[11] *Id.*
[12] http://www.citizenstosaveca.org/release_030805.html (accessed March 10, 2005)
[13] Elections Code Section 9020.

Although election law is generally not the Committee's area of expertise, as it understands it, the process by which petition information is verified by commercial initiative management companies involves checking the signers' names and addresses to determine if the signers are registered voters prior to submitting the petitions to the Secretary of State. This process may involve creating a computer database containing all of the petition information.

According to its web site, Oregon-based TechSpeed, the firm reportedly hired by CSC to verify the validity of petition signatures, performs data entry services using either paper or scanned images. Scanned image files are then sent to the data entry division in India for "content development."[14] TechSpeed's website contains a picture showing an image of a petition and a computer screen with data from that petition entered into a database. (See Appendix following.)[15] It is not yet known how any petition information, if at all, is shared with India, or what if any security precautions were taken in this process.

By creating a computer database of the signers' information, the Indian personal information entry personnel can then compare that information against a separate database of all California voters (called the CALVOTER database) compiled and sold by the Secretary of State on a CD-ROM. According to the Secretary of State's office, the "long form" voter registration information it provides to requesters may includes all of the following personal information about California voters (though it is not clear if any of this information was shared with personnel in India):

- Last Name, First Name, Middle Name
- Address Number, Street Name, Unit Number
- City, State, Zip
- Telephone Number
- Mailing Address
- Language
- Date of Birth
- Gender
- Party
- Status
- Status Reason
- Registration Date
- Precinct
- Registration Method
- Assistance Flag
- Place of Birth
- Previous Registration
- Previous Name
- Previous Residence Address

[14] See http://www.techspeed.com/bin/services-dataentry.php

[15] This image, last accessed on the web by the Committee on March 11, 2005, was apparently removed from TechSpeed's web site on March 12, shortly after the Speaker's announcement of this impending review. The image had been available at http://www.techspeed.com/bin/portfolio/dataentry-projects/images/petitionscreen.jpg.

What Has Been Done With The Petition Signers' And California Voter Information in This Case?

In order to allow for the comparison of the petition signers' database against the voter registration database, TechSpeed reportedly makes the voter registration information available to persons in India where the petition signers' database is created. It is not yet known whether this voter registration information is shipped to India by CD ROM or some other electronic process, or whether it has been shared there at all. Nor is it yet known whether TechSpeed performs this work with its own Indian employees, or whether it hands over the task to one or more other Indian companies or personnel.

A spokesperson for CSC has stated that the petition management firms it hired have some type of confidentiality agreements with TechSpeed that apply to its domestic and foreign employees.[16] However the scope, application and enforceability of these contracts is not yet known, and the contracts have not yet been provided to the Committee for its review. As discussed further below, however, it is unlikely that any relevant contract provisions could be enforced by individual Californians whose personal information may have been affected by this reported international outsourcing of their information. The Committee recently requested CSC, TechSpeed and other related entities to provide the Committee with these and other pertinent documents in order to be able to review what if any protections are required to ensure this voter information does not get into the wrong hands.[17] While the Committee hopes to receive this information, a TechSpeed spokesperson reportedly refused to disclose what was done with the information it obtained because of "confidentiality agreements."[18] It is also not yet known what specific voter or petition information, if any, was outsourced to India by TechSpeed to fulfill its contract with CSC. The Committee has also requested receipt of this information by CSC, TechSpeed and related entities.

CURRENT PRIVACY PROTECTIONS REGARDING CALIFORNIA VOTER INFORMATION

Laws Regarding Petition Signature Information and Registered Voter Data

Petition Information

The privacy protections guaranteed to Californians include protections for voter and petition signature information. In general, the law prohibits the use of petition signatures for any purpose other than qualification of the initiative, referendum, or recall measure for the ballot.[19] Misuse of the petition signatures is a misdemeanor. There do not appear to be civil remedies in statute for violation of this law.

---

[16] Kate Folmar, "Checking Of Voter Data In India 'Outrageous,' Democrats Fume", San Jose Mercury News, March 9, 2005.

[17] The Committee served written requests to appear at the hearing and provide specified information to the co-chairs and general manager of Citizens to Save California, as well as its two commercial petition management companies and the voter data analyst company identified in the media reports.

[18] David Lazarus, "Citizens To Save California Farms A Little Menial Work Out To India", S.F. Chronicle, March 8, 2005.

[19] Elections Code section 18650.

Voter Registration Information

The use of voter registration information is also restricted. Generally, voter registration information is confidential.[20] Limited exceptions exist for political, governmental, journalistic and academic use.[21] Certain voter information, such as a California driver's license or social security number, may never be disclosed to any person regardless of the purpose of use.[22] Violation of these provisions is a misdemeanor.

50-Cent Penalty

In addition to the misdemeanor penalty provided by statute, regulations provide and the application form requires that the data vendors agree to pay to the State of California, as compensation for any unauthorized use of each individual's registration information, an amount equal to the sum of fifty cents multiplied by the number of times each registration record is used by the applicant in an unauthorized manner.[23] Thus it could be argued that currently the cost placed on each of us having our identities potentially compromised at home or abroad is a paltry fifty cents. Moreover, this penalty is paid to the state, not to the individual persons whose privacy was violated. There appear to be no laws specifically providing monetary damages to persons injured by breach of the voter registration information restrictions.

Process for Obtaining Voter Registration Information from the Secretary Of State

The state compiles voter information from the different counties, and provides it to authorized requesters either statewide or by specific counties or districts. A person who wishes to use voter registration information for one of the limited purposes noted must file a written application with either one or more counties or the Secretary of State.[24] Because technological advances have facilitated manipulation of the data, the number of requests for voter information has exploded in recent years.[25]

Counties do not use a standard form for the collection of voter information, and they reportedly do not use a standard procedure for dissemination of that information.[26] Any person who obtains registration information from the state or county may not pass that information on to another person without first receiving written authorization to do so from either the state or county. [27]

Vendors requesting the information from the Secretary of State's office are required to complete an application form in which they acknowledge and agree that that voter registration information will be used only for election or governmental purposes, or research as defined by law. The form further requires the applicant to agree not to "sell, lease, loan or deliver possession of the registration information, or a copy thereof, or any portion thereof, in any form or format, to any

[20] Elections Code section 2194, Govt. Code section 6254.4.
[21] *Id.*
[22] *Id.*
[23] Cal Code of Regs., Title 2, Division 7, Article 1, Sections 19001 through 19007.
[24] Elections Code section 2188; Cal. Code Regs., Title 2, Division 7, Article 1, section 19008.
[25] Secretary of State's Task Force on Voter Privacy, Final Report, June 14, 2004 ("Task Force Report"), at 15.
[26] *Id.* at 8-15.
[27] Cal Code Regs., Title 2, Division 7, Article 1, Section 19005.

person, organization or agency without first submitting a new application and receiving written authorization from the Secretary of State to release such registration information." If the requester is acting as an agent for a third party that is qualified to purchase the data, the Secretary of State's office requires a letter from them, on their letterhead, confirming the relationship and authorizing the agent to purchase the data on behalf of the qualified party. The Secretary of State's office also requires photocopy of identification from the individual who is requesting the data. The Secretary of State's Task Force reported that "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."[28]

OTHER CALIFORNIA PRIVACY LAWS

California's Commitment to Privacy Rights

As noted above, privacy laws generally recognize that protecting individual privacy is good for individuals and good for business. These laws are founded on the principle that respecting individual privacy rights is an essential component to building and retaining public confidence in the marketplace.[29] California has some of the most extensive privacy protections in the country. In addition to the California Constitution, California has also enacted far-reaching statutory protections. For example, the Confidentiality of Medical Information Act (CMIA) and the California Financial Information Privacy Act closely regulate the use and sharing of medical and financial information.[30] The Civil Code also provides for a variety of other protections for and restrictions on the use and sharing of personal information, including restrictions on the public use of social security numbers and disclosures on tax returns.[31] Certain privacy protections specifically restrict the collection, management, and dissemination of personal information by state agencies.[32] Both public and private entities must take safeguards to protect consumer information, and consumers have a right to know how their personal information is used.[33] The law requires businesses and state agencies to inform consumers if a security breach occurs.[34] These laws create a new shield of protection for the privacy interests of Californians. However, as will be discussed shortly, this shield likely loses its protective qualities once any such information of Californians is shipped or shared abroad.

Recent Unsuccessful Legislative Efforts to Improve California Privacy Protections

The Legislature has recently sought unsuccessfully to improve California privacy protections in a number of respects. Perhaps most relevant to the current discussion are the following:

- ✓ AB 2079 (Oropeza) of 2004. Voter privacy. Passed last year by both houses of the Legislature, this bill, among other things, permitted certain voters, including stalking or domestic violence victims and reproductive health care workers, to request that their

[28] Task Force Report, at 13.
[29] California Department of Consumer Affairs, "California Information-Sharing Disclosures and Privacy Policy Statements," at 5.
[30] Civil Code sections 56 *et seq*. and Financial Code section 4050 *et seq*.
[31] Civil Code section 1799.1a.
[32] Civil Code section 1798 *et seq*.
[33] Civil Code sections 1798.81.5, 1798.82.
[34] Civil Code section 1798.81.5.

voter information remain confidential. The bill also required the Secretary of State to study the feasibility of inserting fictitious names of voters into the voter registration information database as a possible investigative and enforcement tool for determining inappropriate or unauthorized uses of voter registration information. Status: Vetoed.

- ✓ SB 1492 (Dunn) of 2004. Outsourcing of medical information**.** Passed last year by both houses of the Legislature, this bill sought to provide patients with the right to control whether or not their confidential medical information is transmitted abroad by prohibiting health care companies from outsourcing individually identifiable health information unless specified requirements are met. Status: Vetoed.

The General Limits of California Privacy Protections Abroad

Initial research by the Committee suggests that regardless of whether the unseen contracts purportedly entered into between CSC and TechSpeed contain confidentiality provisions, it is highly unlikely that California identity theft victims would be able to effectively enforce these contracts in India or any other foreign nation if a breach occurs. First, individuals who are not parties to a contract generally have no right to enforce the contractor to recover damages for breach of the contract. In addition, under traditional rules of statutory construction, there is a strong presumption against applying U.S. laws beyond the territorial boundaries of the United States.[35] For example, the U.S. Supreme Court has held that acts of Congress are presumed to apply only within the boundaries of the U.S., unless the act contains an express intent to the contrary.[36] The underlying rationale of the presumption against extraterritoriality is that it "serves to protect against unintended clashes between our laws and those of other nations."[37] Thus, the logic of the presumption against extraterritorial application abroad would likely apply with even greater force to a state statute. Moreover, because of the importance of speaking with one voice internationally, courts have applied an even more stringent standard to state legislation that applies abroad than to actions by the United States Congress.[38]

The Laws of India Would Not Appear To Protect California Voters' Privacy Interests

The precise contours of Indian law respecting privacy rights are not known. However, commenters have stated that "Indian data privacy laws don't really exist… What India needs to put in place is a mechanism that will protect against the misuse of personal data that is in one's possession rather than misuse of data that is in one's ownership." It has also been suggested to have a "'job hoppers' database to monitor the movement of employees which will, amongst other things, make it easier for companies to track employees who have misused personal data," and to "mak[e] data theft and misappropriation a criminal offence under the Information Technology Act, 2000."[39] Whatever the scope of Indian law might be, however, it clearly provides little

[35] See Extraterritorial Application of the Americans With Disabilities Act, 2 Asian-Pac. L & Pol'y J. 269 (2001).
[36] EEOC v. Arabian-American Oil Co., (1991) 499 U.S. 244 (holding that Title VII did not apply extraterritorially to regulate employment practices of U.S. firms employing American citizens abroad).
[37] Arabian-American Oil Co. at 248.
[38] See Barclays Bank Plc v. Franchise Tax Bd., 512 U.S. 298, 311-12 (1994)(scrutinizing application of California tax law to foreign operations).
[39] V. Kathpalia and V. Parikh, "India Under Pressure To Enact A Data Protection Law", Economic Times, April 11, 2004.

effective remedy for Californians whose rights may be violated by a breach of privacy in India given the practical limitations of attempting to enforce one's rights in a foreign country.

Conclusion: The Facts Remain Elusive What Voter Information Was Outsourced to India and What Risks Petition Signers & Voters Now May Face If This Information Is Stolen

The Committee's review of the facts in this reported case of the potential international outsourcing or sharing of California voter or petition signer information has just commenced. There clearly remain many more questions than answers about this potential development. These questions, which hopefully will be answered soon by the parties who can provide the information to the Committee, include among other things:

1) What voter information, petition signatures or other information was disclosed to or shared with personnel in India, and in what format? If it was so shared, how is that data being used and stored, and retained, by whom, and how was the information transmitted between, or shared between, the United States and India?

2) From what sources was this voter information, petition signature or other information obtained, by whom, in what format, and how was it acquired?

3) Did Citizens to Save California or its commercial petition contractors know that voter data, or petition signature data, or other information would, if it was, shared with persons or companies in foreign countries, and did they assess the risk that any such information could be potentially used to perpetrate identity theft, invasion of privacy or other violations of California law?

4) What if any steps have been taken to protect the security and confidentiality of voter information, petition signature and/or other information that may have been shared with personnel in India? What mechanisms are in place to provide warning in the event of a breach of security or misuse of any potential voter, petition signature or other information that may have been shared, and what if any assurances do California voters have that they would be notified of any breach of security or misuse of such voter information, petition signatures or other information by the persons or firms involved, if any such information was shared with personnel in India?

5) What if any remedies are available to California voters for breach of confidentiality or other misuse of their personal voter information, petition signatures or other information provided by Citizens to Save California or its contractors to firms or persons in foreign countries?