Statewide Databases of Registered Voters:

Study Of Accuracy, Privacy, Usability, Security, and Reliability Issues commissioned by the U.S. Public Policy Committee of the Association for Computing Machinery

Chapter Overviews and Recommendations

Accuracy

Databases are only as good as the data they contain. Quality assurance is a challenge for any database because data entry and necessary merges and purges of data within the system can create errors. Maintaining accurate VRDs is even more difficult considering the mobility of the U.S. population[1] and the wide variety of information sources voting officials must use to verify registration records. Further, voting officials must balance between competing concerns of ensuring that each legally registered voter can cast his or her vote and preventing ineligible voters from casting votes. Accuracy concerns often lie at the center of these debates. An additional complication is that voter eligibility rules are determined state-by-state, and VRD design and implementation are likely to differ state-by-state.

Accuracy Recommendations

Voter Verification

- Voters should easily be able to determine if they are registered.
- Voters should be able to verify that they are registered through the use of a computer or handheld device located at any of the polling places in that state. Responses should not include personally identifiable information about the potential voter.
- Voters should be able to view the relevant contents of their voter registration records to check for accuracy and should be provided with easy-to-use mechanisms and contacts for correcting errors.
- Electronic Election Day updates to registration records are risky and should be implemented only after careful testing, if at all. Paper forms are a well-understood alternative.

Notice

- Whenever a voter or potential voter is determined to be ineligible to vote, the reason and source of information for the determination of ineligibility should be noted in the VRD for the potential voter to review and contest, if appropriate.
- Voters should be notified when their records change in any way that affects their eligibility to vote.
- Public notice of polling places should be provided well in advance of an election (e.g., signs in neighborhoods, prominent notices on local web sites).

---

[1] A recent report of the Commission on Federal Election Reform found that "during the last decade, on average, 41.5 million Americans moved each year."

- Each registered voter in the VRD should be mailed a postcard with his or her assigned polling place and registration status in advance of the election.

Polling Place Lists

- Polling place lists (whether paper or electronic) of all registered voters associated with a particular polling place should be generated automatically by the VRD well before Election Day.
- Automatically generated lists should be carefully checked by at least two local officials and far enough in advance of elections to allow time for corrections.

Archiving

- Ineligibility records should be retained in the VRD for at least twenty-two months and possibly longer.
- If for any reason it is determined that an individual is ineligible to vote, that individual's record should be marked accordingly, not deleted.
- When information is sufficiently old (we recommend at least 22 months), it should be moved from the VRD into an offline archival database that is never purged and is protected against unauthorized disclosure or access.

Other Databases

- When other databases, such as driver registration databases, are used to check for eligibility, those databases should be used for screening and not to automatically enroll or de-enroll voters.
- An automated check can be used to flag some voters for further scrutiny, but the final determination of eligibility should be performed only by an appropriate election official.

Merges, Purges, and Batch Updates

- Large-scale automated database merges are error-prone and should be avoided if possible.
- If purges are performed, they should be done well in advance of any election. People whose names are purged from the VRD should receive notification in sufficient time for them to be able to correct any errors.
- A greater level of authority should be required to perform a batch update than is required to make smaller changes.

Accountability

- There must be well-defined accountability for all changes to the VRD including to source code, database schemas, database contents, and system configuration.
- Changes should require approval or sign-off by an authorized individual.
- It should be possible to identify a clear chain of responsibility for each change, and the VRD should be designed to facilitate tracking of this information.

Audits

- A complete audit trail should log all modifications to the VRD.

Privacy

The public is increasingly aware that personal information in electronic form can pose new risks, such as identity theft, to personal privacy. As state and local governments digitize, centralize, and share this data, the stakes are raised still higher. While VRDs may pose threats to privacy, technology also opens up new opportunities to protect privacy. As governments design and implement these systems, privacy values must be considered a fundamental part of the design process, not simply applied as an afterthought.

Privacy policies for voter registration activities should be based on Fair Information Practices (FIPs), which are a set of principles for addressing concerns about information privacy. FIPs typically address collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

Privacy Recommendations

Openness (Transparency)

- Publish on the main election board website a complete notice of policies and practices describing the collection, maintenance, use, and disclosure of voter registration data. The notice should include contact information for the office or the officials responsible for voter registration data.
- Publish a readable summary notice in other places, such as voter registration forms, at polling places, on sample ballots, and elsewhere as appropriate.
- Provide a copy of the complete notice to any person who requests it.
- Publish any changes to the notice before the changes become effective, and accept and consider public comments.
- Place a date and version number on notices as they are published. Maintain, and make publicly available, copies of all previous notices, including the periods of time during which they were effective.

Data Collection Limitation

- All data should be collected by lawful and fair means.
- Data should be collected, where appropriate, with the knowledge or consent of the subject.
- Registrants and the public should be informed through the published notice of policies and practices of the sources of all data obtained for voter registration purposes.

- The types of data elements to be collected should be subject to public scrutiny.
- Data collection should be limited to sources and procedures authorized by law and properly described in the published notice.
- Only the minimum information necessary for, and relevant to, voter registration purposes should be collected and maintained. The reason for collecting each type of personal information should be explained, and the specific data elements collected should be subject to public scrutiny.

Use and Disclosure Limits

- Limit use and disclosure of voter registration data to activities directly related to the election process or to other activities expressly authorized by law.
- Describe all uses and disclosures in the published notice of information practices. Identify publicly all recipients of voter registration data.
- Provide public notice of and, if possible, a chance for public comment on all disclosures of identifiable voter registration data for any activity not directly required for voter registration purposes.
- Restrict access to specific records, specific data elements, and specific classes of voters (e.g., by location) to those election officials who have a need to use those records, data elements, and classes in the performance of their duties.
- For some or all uses by election officials or disclosures to external parties, maintain a record of the date, nature, and recipient of all personal information and make the record accessible to the data subject upon request.
- Restrict disclosures to specific data elements permitted by law and necessary to accomplish the purpose of the disclosure. Withhold data elements that are not essential to accomplish the purpose of the disclosure or that would place data subjects in excessive jeopardy to identity theft or other improper activities.
- Prevent recipients of data from using or redisclosing the data in ways not specifically authorized by law. Asking recipients to sign data use agreements is one way to accomplish this purpose.
- Allow some non-essential uses and disclosures only with the affirmative consent (opt-in) or negative consent (opt-out) of the data subject.
- For some data subjects at risk (e.g., victims of spousal abuse, jurors, some public officials), it may be appropriate to further limit disclosures.
- Even the best use and disclosure policies may be violated by people and software within the election process. Therefore, limit access by each person and each system component.
- Provide access for every voter to a personalized list of those third parties who have been given or purchased access to his or her voter registration data.

Usability

VRDs will be used in many ways by a wide variety of people. Ensuring that well-trained election officials, minimally trained volunteer poll workers, and voters with little to no technical skills can all use different and appropriate aspects of VRDs is a key challenge for designers of these systems. Poorly designed user interfaces might confuse users or,

worse yet, disenfranchise voters. This can create the reality or the perception of an unreliable system, thereby undermining the entire process.

Usability Recommendations

General Usability

- Consider the various types of users, tasks, and environments in which the voter registration database will be used. Design user interfaces that address all of these factors, providing different interfaces for different combinations as necessary.
- Use accepted user interface design techniques to build data entry forms and data retrieval components that are clear, usable, and interpretable.

Design and Features

- Involve a wide range of test users of different backgrounds, skills, literacy levels, ages, and roles (county official, election volunteer, voters, etc.) in all stages of user interface design, including gathering of usability requirements, design of user interfaces, and testing and evaluation.
- Treat user interface design as an iterative process: use evaluations of user interface designs to guide revisions that themselves can be evaluated in turn.
- Provide informative feedback (i.e., provide users with detail sufficient for understanding the impact of their actions, results of queries, and characteristics of the current operating environment).
- Eliminate unnecessary functionality and data output in favor of simple, minimal user interfaces.
- Provide online tutorials and help systems for all voter registration database user interfaces. For critical applications such as voter verification on Election Day, appropriate experts should be available to help address any concerns.
- Ensure that public-facing interfaces (e.g., World Wide Web based services) are vendor-neutral and are designed to meet widely accepted technical standards.

Evaluation and Testing

- Use a variety of user interface evaluation techniques, including heuristic evaluation by usability experts, “think-aloud” sessions, and user studies.
- Test interfaces thoroughly with representative users performing tasks under situations that approximate those likely to be found in real use.
- Test user interfaces under extreme or suboptimal conditions, including high processor load, network congestion, and noisy or extreme environments.
- Test web-based user interfaces for use by the public on as wide a range of browsers as possible, including multiple older (and pre-release) versions of popular browsers and screen-reader systems for people with visual impairments.
- Evaluate user interfaces, particularly web-based interfaces, to determine their impact on other system goals such as reliability, security, accuracy, and privacy.

Security

Security underpins each of the issues discussed in this report. Maintaining accurate and private information is impossible if a VRD is vulnerable to malicious attack. Further, the validity of data within the VRD may be called into question if the system is easily compromised or lax security policies are established. Ultimately, an unsecured VRD could undermine elections. Good security policies address many different factors. Election officials should establish detailed access controls for each user accessing the VRD, procedures to harden VRDs from attack, and mechanisms to deal with and recover from security failures.

Security Recommendations

Designing & Implementing Access Control Policies

- Federal, state, and local election officials should work together to establish a common framework for access control policies, such as common roles and responsibilities of users and their levels of access, as well as who would be responsible for ultimately implementing and enforcing access control policies.
- Access control policies should not grant the same privileges to all users; rather the policies should group people by established roles and geographic areas. For example, the security policy might give the same level of privileges to all data entry officials for a particular county, but privileges should be different for VRD administrators.
- Access control policies should minimize the number of people who receive privileges both to access each piece of information and to grant access to others.
- Access control policies should ensure that each person is granted only the minimal set of privileges needed to do his or her job.
- Access control policy should cover all records stored in the VRD including records on both voters and non-voters.
- VRDs should use access control mechanisms provided in the database management systems provided; trying to implement access control entirely at the application level leaves greater opportunity for security mechanisms to be bypassed or compromised.
- VRDs should create public logs of all changes to the list of authorized users and their access rights, and any changes to either of these should require authorization from two different persons.
- Authorized users of the system should receive security training, including how to protect passwords and how to resist social engineering attacks (attempts to deceive someone into performing certain actions), and the importance of never sharing passwords.
- Older versions of access control policies should be retained, along with their dates of applicability, and possibly made available to the public to increase the transparency of the system.

Administrative Privileges and Emergencies

- The number of people with administrative privileges for the VRD should be limited; very few users should have the ability to grant access to others.

- People with administrative access should not be allowed to grant themselves new access privileges unilaterally; rather, such a change should require the consent of another administrator.
- Officials should create rules that allow trusted election officials to increase temporarily the privileges available to others during emergencies in a controlled and fully audited manner.
- Emergency overrides should require two-person authorization and generation of detailed audit logs.

Security Metrics

- Those responsible for managing VRDs should measure how effectively they have limited VRD users' privileges by determining how many people have access to how much data and by tracking effectiveness over time using these metrics.
- The EAC or some other appropriate organization should help develop and identify appropriate metrics.

Protecting Against Attack

- All communication channels used by the system should be secured. Anything transmitted over open communication networks, such as any wireless connection, the Internet, or the phone system, should be protected using end-to-end cryptography.
- Firewalls should be used to severely limit connectivity between internal and external networks.
- Mechanisms should be deployed to detect any penetration of system defenses or any insider misuse.

Dealing with Security Failure

- It must be possible to recover from security failures (e.g., retaining historical copies as well as the latest, regular backups with offsite storage, etc.)
- Officials should obtain independent security reviews of the VRD before system deployment and periodically thereafter.
- Individuals should be notified if an inappropriate person may have obtained their data.

Reliability

Because VRDs control access to voting, they must meet a very high standard for reliability. If the system fails, it may disenfranchise voters and undermine public confidence in elections. VRDs should be designed to be reliable both during the non-peak times before and after an election, and for high-activity times such as Election Day. While reliability issues are often considered in terms of “always on” electronic systems, registration systems may be economically designed to employ both online VRD and offline solutions, such as distributing DVD-ROMs of registration data to polling places for use on Election Day. State and local governments should assess the entire scope of

reliability issues and design systems that have built in redundancy, replication, and distribution, but also incorporate mechanisms that allow the voting process to proceed should the VRD fail. States may choose to implement the VRD by centralizing the database at the state level or decentralizing it and spreading responsibility among the different local jurisdictions; officials must recognize that reliability issues differ depending on the chosen implementation.

Reliability Recommendations

Redundancy

- Use redundancy to alleviate failures affecting time-critical operations.
- Ensure that redundancy actually increases reliability by conducting system failure tests.

Replicated Data

- There should be multiple copies of the database.
- Copies should be physically separated to protect against physical damage.
- Copies should be logically separated (i.e., in different forms/types of systems) to protect against software failure and attacks.
- The data on physically separate copies (such as DVD-ROMs) should be encrypted. Encryption and decryption mechanisms should be tested.
- Different channels, including alternate network providers and routes, physical media, and printed copies to access different replicas should be provided.

Distribution

- Evaluate the ability of individual databases to function when other parts of the system fail.
- Evaluate distributed database solutions with respect to their ability to meet the HAVA-mandated goal of a single, uniform, official, centralized, interactive computerized statewide voter registration list.

Centralization

- Evaluate the ability of the system as a whole to respond to the unavailability of one or more copies of the centralized database.

Archives

- All changes to the database that affect the ability of an individual to vote must be logged and archived.
- Archival media, including audit logs and backups, must be write-once or otherwise protected to ensure that accurate records of changes to the VRD have been maintained.

Election-Day Fallback Processes

- Develop fallback processes for registration verification so that elections can proceed even in the face of system failures.
- Ensure that fallback processes will withstand any failure that would not otherwise prevent voting. If a power failure at a polling place does not prevent use of voting machines, then it should not prevent voter registration checks to be performed.

Provisions for Delayed Entry of Registration Information

- Develop processes supporting delayed entry of registrations.
- Analyze the impact of near-deadline registration and early/absentee ballots on the system.

Testing

- A defined and empowered quality assurance group should be in place from the beginning of the project. The group should develop functionality, usability, and reliability tests.
- Periods of peak stress (e.g., immediately before registration deadlines, during elections, and registration verification) should be identified for reliability testing, as should the activity mix during periods of peak stress. Consider questions such as how many simultaneous users or operations are expected, and identify all potential component failures. Testing should check whether system performance will be adequate even when some system components have failed.
- Tests for security against likely attacks (e.g., denial-of-service attacks) should be conducted.