KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

PEW'S UPGRADING VOTER REGISTRATION (UVR) DESIGN: AN ASSESSMENT OF THE PRIVACY AND DATA SECURITY PROTECTIONS

July 11, 2011

Pew's UVR design, and the ERIC data center at its core, incorporate technology, policy and governance features that appropriately balance and advance the interests at stake: improving the quality of voter registration data while at the same time protecting and even improving the privacy and security of information shared across state lines for registration purposes

Introduction and Summary of Conclusions

The Upgrading Voter Registration Initiative (UVR) of the Pew Center on the States (Pew) represents a groundbreaking approach to improving the quality and utility of state voter registration systems, using advanced data sharing and data analysis techniques to improve the accuracy and completeness of voter registration databases while protecting privacy and data security.

As envisioned, the UVR design includes a data center, likely to be called the Electronic Registration Information Center (ERIC), for analysis of voter registration information. The operations of the center will be governed by participating states.[1] Subscribing jurisdictions will submit, at a minimum, their voter lists and state motor vehicle data to the center, where the information will be cross-checked against data from other states and other relevant data sources to compile the most accurate and up-to-date information about registered voters and individuals who are eligible to register. The data and analyses from ERIC will be used by elections officials to update and correct records on voters who have moved, changed their names or died and to remove duplicate and invalid records while facilitating the enrollment of eligible voters. Overall, the goal of the UVR initiative is to achieve cost savings and more accurate and useful information for election officials by taking advantage of economies of scale and data analysis techniques widely used in the private sector.

ERIC, like any system for the collection, analysis and use of information about individuals, poses issues related to the appropriateness and fairness of the use of the data. Those issues can be resolved—that is, information can be exchanged and used fairly and securely—though a combination of system design (technology), policy and governance (oversight and accountability).

---

[1] Our assessment and conclusions are based on the description of the UVR design in the Pew report "Upgrading Democracy: Improving America's Elections by Modernizing States Voter Registration Systems" (April 2011) and on other materials provided to us by the Pew Center on the States Election Initiatives.

The UVR design incorporates privacy principles and technologies that have been adopted and proven effective in a wide range of government and private sector applications. The design centers around a narrowly defined purpose and includes the application of encryption, access controls and audits to ensure that data is properly used for that purpose and no other. As we discuss below, it is contemplated that governance mechanisms will be adopted, based on proven models, to ensure that the system operates in an accountable manner. Moreover, we are very pleased to see that UVR includes a very forward-looking proposal to offer online portals where voters can enter their own registration information and update their records, empowering voters with the means to correct errors or update their information.

The Center for Democracy and Technology (CDT) concludes that UVR, and ERIC specifically, are on a path to being implemented in a way that appropriately balances and advances the interests at stake: improving the quality of voter registration data while at the same time protecting and even improving the privacy and security of information shared across state lines for registration purposes. The UVR design currently incorporates privacy and accountability features that address all elements of the comprehensive privacy and security framework that CDT believes is suited to a system of this nature. Recognizing that the details of ERIC operations and governance have not been fully finalized, we also offer additional observations that may guide the establishment of UVR and its governance structure, consistent with the foundation that has already been laid.

A Privacy Framework for UVR

Pew engaged the Center for Democracy & Technology (CDT) to assess the privacy and data security issues associated with ERIC. In assessing ERIC, CDT used the widely-accepted privacy policy framework known as Fair Information Practice principles (FIPs). In particular, we followed the version of the FIPs adopted by the U.S. Department of Homeland Security (DHS) in 2008.[2] Using the eight principles in the DHS framework, CDT has conducted an assessment of ERIC and has developed the following conclusions and recommendations.

1. Transparency

Any system using information about individuals should publish clear, complete and specific notice to data subjects regarding the processing of personal information in connection with the system. To provide such transparency, the governing body for ERIC will create a website, which will describe each information category or data set that is used within the system as it evolves over time, the source of such information, the rationale for its use, and the periods of time that such information is retained, as well as a description of the information that is reported out of the system to the states or shared with other entities, if any. The notice should be comprehensible to the average voter, but should also provide fuller information useful to privacy and voting rights experts in understanding the system. The website should also provide links to any state-based portals that are created for online registration or data access by voters themselves. The website as planned will also publish the ERIC's bylaws, membership, and other accountability information (e.g., audit reports and sufficient information about the system design and contractor

[2] *See* U.S. Department of Homeland Security, "Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security" (Dec. 2008) http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

relationship to permit outside assessment). Participating jurisdictions should consider whether and how to incorporate notice of ERIC in their own websites and registration materials.

2. Purpose Specification

The purposes of a system processing personal information should be clearly defined. Pew has addressed this principle by making it clear that ERIC would be used solely to improve the quality of voter registration information by providing sophisticated analysis of voter files submitted by the states in combination with other data sources to provide reports back to the participating states to enable those states to identify inaccurate or invalid registration records and eligible but unregistered individuals. Appropriately, this purpose statement is both enabling (i.e., it permits collection, use, retention and disclosure of information for the specified purpose) and limiting (i.e., it prohibits unrelated uses, thus providing insulation against mission creep). Such a clearly defined purpose statement will help the entities developing ERIC and, once established, its governing body and participating states to guide all further decisions about ERIC implementation and evolution.

The purpose specification is referenced in the draft membership agreement with participating states that CDT reviewed. In addition, the purpose specification should be incorporated in the articles of incorporation and bylaws for the entity that will manage ERIC. Any contract with a service provider processing information for ERIC should also include a provision that prevents the contractor from using information in or derived from the system for any other purpose.

We also note that Pew has been clear in another way about the purpose of ERIC, by specifying what ERIC is *not* intended to do: ERIC reports are not a determination of eligibility or ineligibility to vote, and the responsibility for using the analytic reports from ERIC rests with the election officials of the respective states, acting pursuant to applicable law and practice.

3. Individual Participation

Individual control or choice is a feature of almost all privacy frameworks. Several elements of the UVR design would implement this principle.

Sometimes, the principle of individual participation is reduced to a debate over opt-in or opt-out. Neither is a key consideration for UVR, given the laws that already mandate data sharing and verification for voter registration purposes. It is not necessary in our view to allow individuals to either opt-in or opt-out of the transfer of data about them from the states into ERIC. Congress and the states have made policy choices in favor of sharing data to improve voter registration rolls, including data collected for other purposes (such as DMV or Social Security data). To the extent that the purpose specification of UVR remains narrow and is respected in its operations and evolution—that is, to the extent that there are no uses or disclosures of data for any purposes not related to supporting the states in the administration of elections—the individual control principle does not require individual consent to the sharing of relevant data in aid of the voter registration process.

One important way that the individual participation principle is implemented in the UVR design is through the protection against erroneous adverse decisions that will be afforded by the "failsafe" and due process mechanisms afforded by the states. Under state and federal law, states should already have robust procedures for protecting individuals from being improperly removed from

the rolls or from a failure to record a registration that was submitted on time. We understand that these procedures currently include, for example, notice by the relevant authority to an individual before he or she is removed from the rolls. These state-level procedures, if properly designed, should ensure that individuals can obtain correction of errors and prompt redress of erroneous enrollment decisions. The ERIC governing board, in its ongoing evaluation of the system's effectiveness, may at an appropriate time find it useful to consider how reports from the ERIC data exchange and analysis are being used by the states in the context of local procedures for registration decision making and redress.

Another element of individual participation is the ability of individuals to access data held about themselves. We are very pleased to see that UVR includes a very forward-looking proposal for the states to offer online portals where voters can enter their own registration information and update their records. This empowering approach recognizes that individuals are one of the best sources of information about themselves and that they should be afforded a means to correct errors or update their information.

4. Information Minimization

Information systems should only collect, retain and disclose personal information that is directly relevant and necessary to accomplish the specified purposes. This principle is implemented in part in ERIC by the format of the reports to the states, which shall include only the minimum information necessary for the states to make registration decisions. The UVR design specifies that reports to the states will sequester any protected information.

Another way in which ERIC will minimize data collection and retention is to use a technology known as "one-way hashing" to mask certain especially sensitive data fields, such as drivers license and Social Security numbers. Hashing technology is widely recognized as an effective means of protecting sensitive information against misuse while still preserving its usefulness within a system. Under current plans, these sensitive data fields will be hashed before records are transferred to ERIC.

In addition, the UVR design contemplates that data sets used and retained in ERIC will be limited to ones that are considered directly relevant and necessary to accomplish the system mission. It is not necessary to impose a specific data retention period; rather, different types of data of different ages may be relevant and necessary to fulfill the specified purposes. However, plans are for the ERIC governing body to establish a data retention policy and purge data that is no longer useful. Further, the ERIC governing body will regularly assess the utility of its analyses and reports, in order to determine if all of the information being collected and reported is in fact relevant and necessary and to adjust system inputs or outputs to avoid unnecessary collection, retention or disclosure.

5. Use Limitation

As a general principle, data collected for one purpose should not be used for other unrelated purposes. In the UVR design, this principle is implemented though an express provision in the membership agreements with the states specifying that ERIC's data and analyses will be used only for the purpose of assisting the states with their administration of elections. The ERIC design includes appropriate identification and authentication controls for employees who have

access to data and auditing mechanisms, which will further serve to enforce the use limitation principle.

6. Information Security

Any information system should protect personal information through appropriate technical, physical, and administrative safeguards against the risk of loss, unauthorized access or use, destruction, modification, unintended or inappropriate disclosure, or interruption of availability.

The ERIC design addresses the information security principle by calling for the use of the same level of security protocols used in the private sector for similarly sensitive information, including the adoption of proven encryption technology. In particular, the ERIC design anticipates that sensitive data (such as drivers' license and Social Security numbers) will be protected by one-way hashing) before being entered into the system so that it can be used in the matching process but not stored in a readable form or disclosed in system outputs. We recommend that encryption be used on data in transit and, as appropriate, on data in storage and we understand that such techniques are planned for ERIC.

The ERIC design also anticipates the application of well-accepted mechanisms that restrict access to a limited number of authorized users, each authenticated in a unique way, to control user privileges and to allow tracking and auditing of all actions taken in accessing or altering data.

7. Information Quality

Personal information used in any system should be reasonably accurate, relevant, timely, and complete for the specified purposes, and there should be reasonable confidence that the outputs of the system are reliable. This principle does not require complete accuracy in either the data used by any system or its outputs. Instead, it requires an entity to consider the quality of the data it uses and to use only data that is reasonably accurate, relevant, timely and complete in light of the purposes for which it will be used. In addition, when it comes to name matching and the process of resolving ambiguities in databases of identifying information, the data quality principle must be applied in light of advanced data analysis techniques that are able to produce highly reliable results by combining data sets that are themselves not highly accurate, timely or complete.

The ERIC design builds on these advanced techniques of data analysis, which are able to yield highly reliable results with data of varying degrees of currency or accuracy. In addition, the ERIC design contemplates fine-tuning of the analytic processes to accommodate the strengths and weaknesses of source data. Application of the information quality principle must recognize that ERIC will be receiving voter registration data from the states "as is," and it is a primary purpose of the system to improve the quality of that data. Moreover, to the extent that state or federal law requires that certain other governmental data be matched with voter registration data, ERIC cannot decline to include that data in its processes. However, the data quality principle does apply to the other data that will be drawn into ERIC from non-mandated government sources or from commercial sources to be matched with the voter data. With respect to that range of data, the purpose of the information quality principle is to encourage the ERIC developers and governing body to assess potential data sources, both before they are accepted into the system

and periodically thereafter, to help ensure that the "discretionary" data inputs being used are adding to the quality of the results.

8. Accountability

Sound usage of an information system should be ensured through mechanisms for regular auditing and evaluation.

ERIC's design calls for its processes and systems to be monitored and auditable. The UVR governing body should ensure that the system implements both technology tools and human oversight to produce regular reports about the workings of the system.

One of the most important elements of accountability already incorporated into the design is the use of comprehensive audit logs in combination with the identity management and access controls discussed under the security concept.

The design further calls for the ERIC governing body to implement a system of independent audits over the controls for personal information and the performance of its operations. The governing body should have procedures to address any complaints that are brought to its attention regarding ERIC analyses.

Oversight and Governance

To ensure adherence to the privacy and data security principles discussed above, Pew is planning a robust governance mechanism through which the participating states will control ERIC. By binding the ERIC service provider and the participating state entities to certain policies, the governance structure can help ensure that privacy is protected both at the outset and as the system grows.

CDT examined a number of organizational structures, policies and standards currently in use by entities that maintain protected personal data, to evaluate their relevance to the UVR. We recommended and are pleased to see that ERIC will be governed by a 501(c)(3) non-profit organization with articles of incorporation, bylaws, a board of directors, and a separate technology and privacy advisory committee. In addition, each state participating in ERIC will sign a membership agreement with the governing body, binding them to a common set of standards to protect privacy and security.

Articles of Incorporation and Bylaws

As a non-profit corporation, ERIC governing body will have a set of articles of incorporation and bylaws. A crucial clause in all articles of incorporation, and an especially important one for ERIC, will be the statement of the purpose. To avoid mission creep and to resist demands to repurpose ERIC data for other uses, ERIC's documents should include express statements of purpose that are narrowly drafted.

The bylaws, which define the procedures by which a member state can withdraw from ERIC, might specify what happens in the case of withdrawal to the data previously submitted to the system by that state. In commercial data sharing or data processing

agreements, it is often a key contract term that, when an entity withdraws, it can be assured that its data will no longer be used or retained. In the case of ERIC, its governing body should consider whether, if any member withdraws, there should be a verifiable process for ensuring that its data, to the extent that it can be re-segregated, is removed from use by the system and deleted from the ERIC's records (subject to any necessary logging for accountability purposes).

Membership Agreements

In addition to bylaws, membership agreements will strengthen the security of the ERIC system. These agreements are critical because they will bind each state, in its participation in and use of data obtained from the system, to abide by the privacy and other policies developed for ERIC. The design calls for participating states to sign agreements defining the responsibilities of each party (the participating state and the ERIC governing body) and incorporating key elements of the ERIC bylaws.

Contracts

As a legal entity, ERIC would be able to use contracts to structure its relationship with other entities. The most important of these will be the contract with the software, hardware, and services entities the ERIC governing body decides to engage. Those contracts should define the vendors' responsibilities, including their responsibilities for protecting the information they receive and process on behalf of ERIC.

Operating Policies

In addition to the organization's articles of incorporation, bylaws, and membership agreements, the governing body for ERIC will need to develop a set of detailed policies for the system. There are a number of the models that may have relevance to Pew and the states as they develop and implement ERIC. For example, the RISS system for law enforcement information sharing has a privacy policy intended to address the proper handling of personal information housed in resources operated by the RISS Program to safeguard the rights of individuals.[3] Materials on the Prescription Monitoring Information Exchange (PMIX) may be relevant to ERIC as well.[4] For example, under the proposed architecture for the PMIX, personal information will remain encrypted while passing through the hub, and no state data will be stored in the hub.[5] And the preeminent source of guidance on establishing systems for the exchange of health information is the Connecting for Health Common Framework.[6] The Framework, developed as part of a public/private collaboration organized by the Markle Foundation, provides a comprehensive set of model policies, technical specifications, and contract language for health information networks.

---

[3] http://www.riss.net/Privacy.aspx. In addition, the six RISS centers operate under the Criminal Intelligence Systems Operating Policies, 28 C.F.R. 23, http://www.access.gpo.gov/nara/cfr/waisidx_01/28cfr23_01.html.

[4] http://www.ojp.usdoj.gov/BJA/grant/10PDMPFAQ.pdf.

[5] http://www.pmpalliance.org/pdf/ASPMP_PMIX_Pres_0410.pdf.

[6] http://www.connectingforhealth.org/commonframework/. The Connecting for Health framework has been tested since 2005 in three states, California, Indiana, and Massachusetts, and is also being used by the federal government in developing the Nationwide Health Information Network.

Transparency

Given the public sensitivity that exists both around voter registration issues and around the centralized use of identity information, we believe that transparency, and open meeting laws specifically, could be crucial in establishing and maintaining public trust in UVR and ERIC. Many of the states participating in ERIC have open meeting laws and open records laws. It could be a source of criticism of ERIC if its members were seen as drawing behind closed doors matters that would otherwise be subject to public scrutiny. Of course, contract discussions, personnel decisions, and other matters requiring confidentiality would be exempt from any open meeting provision.

The ERIC bylaws include transparency measures such as open meetings of the ERIC membership and publicly available minutes and records. If feasible, meetings of the ERIC board should also be open to the public, consistent with legitimate needs for confidentiality.

Advisory Committee

As an incorporated entity, ERIC will have a board of directors that will play an important role in developing and overseeing ERIC privacy controls. Most inter-state information sharing organizations are governed by boards composed primarily or exclusively of state officials.[7]

The ERIC governing entity would benefit from ongoing counsel from non-governmental experts in the fields of data privacy and security. Therefore, we are pleased to see that the ERIC governing body will create separate advisory committees made up of non-governmental experts in the fields of privacy and technology.

Conclusion

CDT concludes that the UVR design, and the ERIC data center at its core, incorporate technology, policy and governance features that address all elements of an effective and comprehensive privacy and security framework. With these features, UVR and ERIC are on a path to being implemented in a way that appropriately balances and advances the interests at stake: improving the quality of voter registration data while at the same time protecting and even improving the privacy and security of information shared across state lines for registration purposes.

For further information, contact: James X. Dempsey, CDT, 415-814-1712, jdempsey@cdt.org

[7] *See, e.g.*, Criminal Justice Information Service, Bylaws for the Criminal Justice Information Service (CJIS) Advisory Policy Board and Working Groups (2009), on file with author. Nlets also uses a regional structure: states are clustered into no more than eight regions, and each region elects a representative to the Nlets board of directors. *See* Nlets Bylaws, chapter 4 (2005)