BallotPoint Vote-Secrecy

Introduction

Title IV of the LMRDA requires that any vote cast *"…by ballot, voting-machine, or otherwise…"* must be *"…cast in such a manner that the person expressing such choice cannot be identified with the choice expressed."* This means there cannot be any way for someone to link a voter to a vote. ***The BallotPoint design guarantees this!***

BallotPoint has been specifically engineered to comply with Title IV of the LMRDA. That doesn't seem to be the case with other voting systems. A voting system developed to meet lesser standards, such as K-12 voting, home-owners association voting, etc., relabeled with "trust us" will not meet the test. BallotPoint was designed from the ground up to meet the test of the secret-ballot process as defined by Federal Law – it wasn't an afterthought.

Assurance of voter secrecy is complex to engineer and difficult to achieve. We are so confident in our approach to meet the secrecy dictates of Title IV we applied for and were granted a patent on the BallotPoint voting system. What follows is a brief description of how the BallotPoint system assures secrecy.

How can Vote-Secrecy be Guaranteed?

With BallotPoint, votes are secret, because member identity is secret – it's that simple. Votes are not linked to voter identities and then separated at a later time. In the BallotPoint system there is ***never*** an association of name (or identity) with a vote.

There are two secure computer systems that make up the BallotPoint voting system. A proprietary software protocol restricts the transfer of any information between the two systems that could potentially link a voter to their vote.

The two computer systems are: the MRNS (Member Registration and Notification Server) and the ES (Election Server).

Simply put, the MRNS houses member-identifying information (public member ID, name, address, etc.) and the ES houses election-specific information (election questions and answers, member anonymous login-credentials, and votes).

Member information is physically and logically separated from vote information such that no one, not even BallotPoint engineers, can ever connect the identity of a voter with the contents of his or her vote.

*Due to the **physical** and **logical** separation of the two systems, there is no method available for someone, including BallotPoint personnel, to link member-identifying information to votes.*

Physical Separation

The MRNS and ES physically reside in separate facilities.

The MRNS is owned by BallotPoint, but located in a secure, offsite facility owned and managed by an independent third-party. The same facility, which is monitored 24x7, houses computers conducting financial transactions, as well as computers storing litigation documentation, HIPA-compliant medical records, and computer systems operated by departments of the federal government. Access to the facility is controlled and logged by palm-scan and cardkey, and physical access to the MRNS itself requires the use of two keys – one kept by BallotPoint and the other by the third-party that owns the facility. All physical access to the MRNS is logged. No one can access the MRNS without both parties present and the event being permanently logged.

The ES is located in the secure facility operated by BallotPoint. Two different password-protected keyless entries are required to gain access to the ES. Even with access, no information is available to link a voter to a vote.

Logical Separation

No programmatic method exists allowing member-identifying information on the MRNS to be joined with vote information on the ES. A carefully designed software protocol prevents such information from being passed between the two systems.

All application software on the MRNS is written by BallotPoint, but installed only by the independent third-party from an encrypted CD provided to them by BallotPoint. Installation can only take place over the secure web; application software installers never physically access the MRNS. No application software is modified or added to the MRNS in any other way.

Installation of MRNS software by BallotPoint is neither permitted nor possible. This discipline provides a complete-from-day-1 archive, maintained by the third-party, of every application software change ever made to the MRNS. In the event of any investigation, this code-record may be reviewed by a competent authority to verify that the MRNS has always protected member-identifying information.

Public Member IDs vs. Private Voter IDs

The identification numbers an organization knows its members by is considered public information and therefore cannot be used by BallotPoint as any part of identifying credentials allowing access to the voting system.

The MRNS assigns random, 7-digit voter identification numbers, or VINs, to members when voting rosters are uploaded by the organization to the MRNS. The VIN for a given member is stored in the MRNS along with name/etc., but the MRNS provides only a list of VINs eligible to vote in that election to the ES, with no member-identifying information.

VINs are never known by anyone outside of the member and BallotPoint. As previously discussed, there is no way for BallotPoint to tie a VIN to a member, and hence their vote.

Summary

The design of the BallotPoint system guarantees vote-secrecy. Essential aspects of this design are:

- Physical separation of servers – one storing member-identifying information and the other storing election-specific information and votes.
- Software protocol that logically separates member-identities from votes.
- Independent third-party installs software updates on the server storing member-identities.
- Permanent archive of all software updates for server storing member-identities.
- Availability of software protocol and application software for review, if warranted, by a competent authority during an election investigation
- Random voter identification numbers known only to member.
- No method exists for anyone, including BallotPoint personnel, to ever link a voter to a vote.
- ***There has never been a successful challenge to the BallotPoint voting system.***

There exists extensive, permanent audit trails showing physical access to the server housing member identity information, software archives showing all updates from day-1, logs viewable by administrators and observers that show administrator activities, and logs viewable by the member that shows all activity on the member's account.

BallotPoint has been specifically engineered to comply with Title IV of the LMRDA. We are confident that the BallotPoint voting system fully complies and for this reason we guarantee our clients that if there is an election challenge to the BallotPoint system and if, after investigation, the Department of Labor concludes that the election must be rerun due to a finding that the BallotPoint system did not comply with Title IV, then we will remedy the situation and rerun the election under the supervision of the Department of Labor at no additional cost to the union.

This is our guarantee that we adhere to the secret ballot process.

