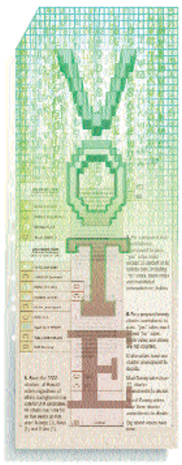
REPRESENTATION OF THE PEOPLE ACTS
GOVERNMENT ELECTION & GREATER LONDON REFERENDUM
OFFICIAL POLL CARD
ON THAMES
2
ROYAL MAIL
POSTAGE PAID
KINGSTON
UPON THAMES
SERIAL No. 58
resident
Vote for one
Vice
Vote

By Rebecca T. Mercuri and L. Jean Camp

The Code of Elections

The disparity between the code of election law and the code that comprises election equipment reflects inherent problems in the translation of social policies into computer procedures and overseeing processes.



Elections are governed by intricate and voluminous codes of laws that, in turn, are (at least in part) transformed into the program code that governs the functionality of computer systems used in election processes. Voting systems reflect the interaction of technology and governance as grounded in the history of democracy in the locality (country or municipality) in which they reside. Variances of election law are therefore as great as the differences in history of democratic nations and states. There are huge (and possibly insurmountable) vagaries of election law, there are assumptions in the law with respect to risks pertaining to technology, and there does not exist any one-to-one correspondence between computer code and natural language documentation (no matter how flawless such documentation may appear to be). It is therefore inevitable that some latitude in legal code be taken in the construction and implementation of computer voting code. This latitude may subsequently hold serious consequences for the ability of the resulting computational system to accurately transcribe the intentions of the voters and to convey this into an appropriate summation of vote totals.

All technology is developed and diffused within a fluid social context. When the social and technical context of the designers is far different from those of the users, gaps will exist where seemingly benign decisions by the creators of the technology may be inappropriately exploited. Voting technology is diffused in a context where the governmental parties in a democracy may have strong and vested interests in the reliability of the technology, or alternatively may wish to ensure that the technology can be allowed to be subverted to favor certain groups or individuals. Technology may be designed to solve a problem, but instead exacerbate it. This was seen earlier

• ILLUSTRATION BY JEAN-FRANÇOIS PODEVIN •

THE CENTRAL IMPORTANCE OF VOTING IN A DEMOCRACY IMPOSES A GREATER NEED FOR OVERSIGHT IN ENSURING THAT THE TECHNOLOGY DOES NOT PLAY A ROLE IN AFFECTING OR THWARTING THE CHOICE OF THE CITIZENS.

this year in India, where electronic voting was introduced with the intention of resolving issues related to paper ballot-box stuffing and ballot removal, but instead the new systems actually made it easier for partisan operatives to commandeer and control entire polling booths. The central importance of voting in a democracy imposes a greater need for oversight in ensuring that the technology does not play a role in affecting or thwarting the choice of the citizens.

In computerized voting, decisions intended to assist the voter can remove critical choices. Overvoting and undervoting are examples of actions, generally viewed as undesirable, that can be effectively prohibited or reduced by election system designs. Overvoting involves selecting more choices than permitted in a particular race, but since the code of laws in many democratic elections does not allow for proportional balloting (casting a percentage of one's vote to different candidates), the prevention of overvoting may deny a citizen the right to protest the lack of a single viable candidate by deliberately choosing more than one (even though it is known that such choices will be discarded). Similarly, write-in votes are often used to make such a statement, but this message may also not be conveyed, because election officials may ignore these inputs entirely if there are insufficient numbers to change the election outcome. Similarly, making it more difficult to skip a race entirely (undervote) can potentially deny the right of the voter to quickly make only a few selections from an otherwise lengthy ballot.

Lessig explains this counterposition of code and its application or use in terms of four constraints: architecture, market, law, and norms [5]. These constraints, or regulators, must remain balanced to result in reasonably acceptable regulation or control. If a breach of constraints using software programming could be illustrated to have caused an alteration or loss of votes, this should initiate protections under election law. The traditional remedy (eventual conviction of the violators) will be incapable of restoring the votes thus lost, so the goal of the perpetrators may be achieved nonetheless. Thus, the law and technology together create a deficiency in norms. It has been long understood that computer science theory is incapable of determining, without a doubt, that software performs certain tasks and no more. Similarly, law written for one context may be found to be ineffective in overcoming inadequacies within a technological architecture.

Code as Social Construct

Computer code (software) is both a sociological and a technological construct. In fact, code is considered a form of persuasive speech by courts, social theorists, and technologists. The question of code as speech has been the subject of numerous U.S. District and Circuit court cases, particularly involving limitations on First Amendment rights to free expression as a result of Federal restrictions over the exportation of encryption software [3]. As well, litigation involving copyright protections and electronic communications asserting First Amendment rights has increasingly viewed digital embodiments as protectable containers and conduits of performances and written works. The case of *RIAA v. Verizon* [12], for example, extends First Amendment rights to anonymous communications (which might, though not in that lawsuit, include private ballot casting) involving data transfers.

If code is indeed speech, and indeed persuasive through design or failure of usability, what is the appropriate oversight needed to ensure correctness? Appropriate oversight depends on an understanding of code in social context. Recognizing code as social construct and as speech results in three possible views of the origin of social bias in code: as technologically determined, as socially constructed, or as the result of dialogue. These views respectively suggest that standards should be created to focus upon: engineering design controls, protocols related to social values, or a continually evolving and iterative monitoring process. Understanding the problems and promises of digital voting in each realm requires both technical acumen and an appreciation of distinct policy regimes. Election officials have tended to view the technology as rigid and determinant, and scientists argue that the technology is fluid and can be subverted—both stances must be understood for risks to be mitigated.

Persuasive controls can be applied positively or negatively, deliberately or inadvertently, obviously or subtly in the design of user interfaces. Certain voting interface implementations have been found to be intuitive to computer users while incomprehensible to novices, or conversely, helpful to novices but overly cumbersome to experienced users [8]. The digital divide that exists between rich and poor, young and old, and majority and minority now extends to the polling place, such that inherently intimidating technology may even serve as a modern-day "literacy test" [7]. Adaptive interfaces may not be feasible or even desirable in the rapid, one-time use setting of the voting booth because of the difficulty of design and verification. Even outside of the polls, disparate access to technology may limit the ability of groups of citizens to register to vote, apply for absentee ballots, and view instructional materials about the election equipment.

Computer software is unique in the history of technologies because the choices imposed by it are not limited by physics. This suggests that social feedback in design can play a larger role than is the case with more constrained physical products. The same is true with election systems, as illustrated by the fact that some electronic voting products used in the 2003 California Gubernatorial recall election reported less than 1% of missed (or "undervoted") choices in the yes/no recall question, but nearly a 10% undervote in the candidate selection for Governor [9]. The insertion of a computational system between the voter and the voter's ballot may thus influence the decision-making process. It is this coercive or persuasive imposition on the voter that must be better understood, particularly within a cultural context.

An electronic system cannot make an automatic distinction between failures in human interaction and an actual attack; in either case, some transactions might be prevented or unauthorized access may be allowed. Electronic intervention to preclude inappropriate election system use can have serious consequences on the validity of the outcome, if applied too strictly (as in the case of broad purging of supposed felons from the voting rolls in Florida) or in too lax of a fashion (thus allowing people to vote "early and often"). Further problems may ensue if underlying code (such as operating system components) subverts the applications software riding upon it. The traditional solution to these types of transactional problems is to provide detailed audit logs that carefully track each user. Yet such logs, even if effective in order to detect tampering or equipment malfunction, cannot be created in voting systems without potentially violating privacy or producing artifacts that could be used in vote selling.

Such issues aside, ultimately election security involves the creation of trustworthy voting systems, with requirements of perfect performance, policies, and practices, which are typically unachievable in actual use. Expectations of perfection (or even near perfection) are inevitably doomed to failure regardless of technologies employed. A secure system can be considered trustworthy in the narrow sense that no data is altered, accessed, or produced without authorization, such that its use can be deemed reliable [2]. In other words, "every vote must count" within margins of error that do not affect the result. In most other endeavors, answers falling within the margin of error call for a "do over"—whereas in elections, a winner or loser must still be declared (even using a coin toss in the case of a tie). Thus, vote counting is inherently problematic, even when chad is neither hanging nor pregnant. Legal code and social norms overseeing the physical custody of voting records are critical, whether the item is a stack of paper or a storage device. Recounts of paper typically require multiple observers, but if collusion or disruption occurs, results may be questioned. Digital recounts that cannot be independently verified are equally questionable. If a system containing both paper and electronic records produces different totals, the determination of correctness may not be straightforward. In these situations, laws and other customs may be required to prevail in dispute resolution.

Procedural Vacuums

The claim has been that the closed nature of Independent Testing Authority (ITA) examinations, combined with trade-secret protections on software code, are acceptable because the certification process ensures that the resulting equipment is safe. Yet substitution of new election tabulation and ballot casting code without recertification has been found to be commonplace, with this practice dating back decades to the earlier paper-based, machine-counted balloting systems. The failure to apply required protocols resulted in the exposure, in 2004, of the use of uncertified software (by Diebold in California and ES&S in Indiana) in election equipment and actual elections. Such alterations have been deemed "necessary" to allow for "bug fixes." Even if it were possible to create perfect code that would function in all possible environments, any changes in election law may then need to be reflected in new computer code, so updates are inevitable. The currently imposed norm is vague regarding procedures that need to be followed to ensure recertification, and also configuration control and management when modifications are applied. At present, it is not readily determinable (except perhaps only by the vendors) whether or not a voting system actually contains an appropriately certified code set, or if its code is trustworthy in the current setting. As well, there is no general process for decertifying a voting system or model if it is determined to be flawed, nor for propagating patches to all products of the same type. Again, the elements of a trustworthy system—transparency in the legal sense and reliability in the technical sense—are in conflict. The result of this conflict is protocol-based protection that cannot be relied upon to provide sufficient assurances of correctness.

THE NORMS AND LAWS OF VOTING PROCESSES HAVE TRADITIONALLY BEEN BUILT ON THE ASSUMPTION OF PHYSICAL BALLOTS.

Those familiar with the history of certification of telephony equipment may find historic irony in a recent Florida ban on simple plastic templates with holes that can be used by the visually impaired or illiterate to vote without assistance. In an earlier classic case, the Federal Court had to intervene to allow Hush-a-Phone to sell small plastic cups to attach to telephones when AT&T objected to such interfering devices as part of their phone system (*Hush-a-Phone Corporation, et. al.*, 20 FCC 391,19550, 238 F. 2d 266, D.C. Circuit 1956). For voting, there is no certification process for small plastic templates, so these can be prevented from use under the caveat that the design of the standards governing certification assumes a specific technology, and that any technology violating those assumptions simply cannot be certified. Similar problems in some regions have thwarted requirements for voter-verified audit trails (such as printing out paper ballots that are viewed by the voter for correctness and then deposited in a secured box, to be used as a check against the computer election tallies) [6]. Paper trails are necessary to resolve otherwise conflicting simultaneous requirements of auditability and anonymity in voting applications, which preclude the use of traditional methods of transaction recording. Plastic devices may be needed to enable segments of the population to vote independently. Yet, as noted earlier, a dichotomy that declares technology as consisting of either only paper or electronic records cannot necessarily accommodate or even mitigate the risks of a merger of both formats. In voting, as in telephony, a narrow literal view of legal code has resulted in irrational rejections of technology.

In the interpretation of legal code, semantics come into play and are currently under debate in the courtrooms. Can the voter-verification concept be applied to a transient image on a computer screen, or must it be provided only in a tangible and immutable record? Is it possible for voters to have sufficient confidence in a cryptographically based system whose underlying mathematics has been deemed correct by a group of experts (especially if the code is also posted on the Internet for all to see)? What is the meaning of a "recount" when a voting system produces only a reprint of internally calculated totals? This last issue has been raised in the Florida courts via Circuit and Federal cases filed by Congressman Robert Wexler of Palm Beach County (*Robert Wexler vs. Theresa LePore, et al.*, No. 4D04-918), claiming a lack of equal protection between touch-screen and optically scanned balloting counties as applied to recounts in the state. An earlier lawsuit involving the lack of equal protection, due to the use of the prescored punch-card ballots by minority population municipalities, failed to succeed in stalling California's Gubernatorial recall election [11]. The issue of whether paper ballots may disenfranchise voters who cannot see them continues to be raised by certain disability activists despite the U.S. Department of Justice opinion indicating that the equal access requirement should not mandate that all voters use the accessible balloting devices, and that the accessible devices should not be exempt from independent audit requirements [1].

Swap the Vote

The norms and laws of voting processes have traditionally been built on the assumption of physical ballots. Physical ballots can be manipulated one at a time locally; however, parallel remote alteration is not possible. Blank physical ballots can be examined in advance, without the need to address emergent failures as long as procedural controls are in place. Practices of watching and observation that provide transparency in paper-based systems do not necessarily extend well to computerized systems and vice versa. Voting equipment purchases have run ahead of the ability of the election community to govern such machines. The interjection of $3 billion of funding under the Help America Vote Act (HAVA), for new U.S. voting equipment, was intended to be regulated by a commission headed by the National Institute of Standards and Technologies, yet the $30 million allocation needed to perform this overseeing work has yet to materialize.

Federal election initiatives, such as HAVA (written into law as a direct result of the Florida 2000 Presidential election controversy and the subsequent malfunction of new election equipment in that state during 2002), the U.K.'s remote voting project (intended to promote turnout), as well as Ireland's attempt to computerize its national elections by 2004, have all met with resistance. These legal solutions seek to resolve organizational, economic, and political problems with technology that cannot be independently validated as unbiased. Under such conditions, the proposed technology inevitably fails, in the larger sense, to solve the underlying issues that caused the initiatives in the first place. For example, the new voting technology does not ensure usability. There is nothing in HAVA that prevents a touch-screen voting machine from displaying a butterfly-ballot layout, as was used with South Florida's earlier punch-card systems. New technology introduces new problems—such as when color and voice capabilities may be subtly persuasive. The problems of digital voting are due to a combination of technological utopianism and a lack of technology-neutral definitions of social barriers, resulting in an organizational inability to perform an unbiased examination of how and when technology can best be applied.

Future Prospects

As the technology is incapable of meeting false hopes, experts are finding themselves in a variety of roles, from guru to skeptic. Indeed, voting technology is following the same cycle as radio broadcasting, Internet commerce, telephony, and many other significant innovations [10]. First there is hope is that the technology will solve all problems. Then comes despair at the failure of the technology to meet the impossible promises of its most zealous supporters. Finally, a regulatory response occurs in order to address technology as embedded in society.

Hopefully, the ongoing discussion between and within the scientific and election communities can be harnessed to developing consensus that can be translated into better products and procedures, rather than (as some have asserted) being harmful by raising undue fears among the electorate. For example, the Internet could be used to distribute ballot designs and layouts for checking by "many eyes" for fairness, usability, and correctness.

Thankfully, science has a way of proving its legitimacy in the long run, and democracy has a habit of finding balance. It took the sinking of the Titanic for governments to require that telegraph operators respond to signals from competing brands of equipment [4]. Hopefully, no such memorable disaster will occur before the new codes of election law, the codes implemented by technologies, and the processes that regulate them all have a chance to be corrected and stabilized. Only then will a truly new and improved breed of voting systems, deserving of the trust placed upon it, be able to begin to demonstrate its merit.

References

1. Bradshaw, S. Whether certain direct electronic voting systems comply with the Help America Vote Act and the Americans with Disabilities Act. Memorandum Opinion for the Principal Deputy Assistant Attorney General, Civil Rights Division, October 10, 2003; www.usdoj.gov/olc/drevotingsystems.htm.
2. Camp, L.J. Design for trust. In *Trust, Reputation, and Security: Theories and Practice*. R. Falcone, Ed., Springer-Verlag, 2003.
3. Camp, L.J. and Lewis, K. Code as speech: A discussion of *Bernstein v. USDOJ*, *Karn v. USDOS*, and *Junger v. Daley* in light of the U.S. Supreme Court's recent shift to Federalism. In *Ethics and Information Technology, Volume 3*, Kluwer Academic Publishers, 2001.
4. Douglas, S. *Inventing American Broadcasting 1899–1922*. Johns Hopkins University Press, Baltimore, MD, 1997.
5. Lessig, L. *CODE and Other Laws of Cyberspace*. Basic Books, 1999.
6. Mercuri, R. A better ballot box? *IEEE Spectrum 39*, 10 (Oct. 2002); www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html.
7. Mitrou, L., et al. Electronic voting: Constitutional and legal requirements, and their technical implications. In *Secure Electronic Voting*, Dimitris A. Gritzalis, Ed., Kluwer Academic Publishers, 2003.
8. Roth, S.K. Disenfranchised by design: Voting systems and the election process. *Information Design Journal 9*, 1 (1998); www.decadeofbehavior.org/policyseminars/er_roth1998.pdf.
9. Shelley, K. *Statement of Vote, 2003 Statewide Special Election, October 7, 2003*. Certified in Sacramento, CA, November 14, 2003; www.ss.ca.gov/elections/sov/2003_special/contents.htm.
10. Spar, D. *Ruling the Waves: Cycles of Discovery, Chaos, and Wealth, from the Compass to the Internet*. Harcourt, 2001.
11. *Southwest Voter Registration Education Project et al. v. Kevin Shelley and Ted Costa*, No. 03-56498 D.C., No CV-03-05715-SVW; Per Curiam Opinion filed September 15, 2003, and subsequent ruling from rehearing by the United States Court of Appeals for the Ninth Circuit, filed September 23, 2003; www.ca9.uscourts.gov.
12. United States District Court for the District of Columbia. Memorandum Opinion in Civil Action No. 03-MS-0040 (JDB), *Recording Industry Association of America v. Verizon Internet Services*, April 24, 2003.

Rebecca T. Mercuri (mercuri@acm.org) currently holds a research fellowship at the Radcliffe Institute of Harvard University where her work focuses on transparency and trust in computational systems.

L. Jean Camp (jean_camp@harvard.edu), formerly of Harvard's John F. Kennedy School of Government, is an associate professor of Informatics at the University of Indiana.