2008

Open Code Governance

Danielle K. Citron
Boston University School of Law

University of Maryland School of Law
Legal Studies Research Paper
No. 2008 - 1

Open Code Governance

Danielle Keats Citron

UNIVERSITY of MARYLAND SCHOOL of LAW

Open Code Governance

Danielle Keats Citron†

The legitimacy of the administrative state has troubled courts and scholars for many decades.[1] Reformers have pursued several approaches. Public participation allays concerns that agency policymaking excludes divergent perspectives and may partially substitute for direct democratic control.[2] Strong oversight by politically accountable actors enhances the democratic

† Associate Professor of Law, University of Maryland School of Law. The comments of Richard Boldt, Maxwell Chibundu, Samir Chopra, Karen Czapanskiy, Martha Ertman, Lisa Fairfax, Susan Freiwald, Jon Garfunkel, James Grimmelmann, Paul Ohm, Frank Pasquale, Ari Schwartz, Rena Steinzor, David Super, Greg Young, and the participants in the *University of Chicago Legal Forum's* "Law in a Networked World" symposium greatly improved this Article. Adam Coleman, Alice B. Johnson, and Susan McCarty provided excellent research assistance. Dean Karen Rothenberg and the University of Maryland School of Law generously supported this research. I thank the editors of the *University of Chicago Legal Forum* for their superb assistance.

[1] See, for example, Richard H. Pildes and Cass R. Sunstein, *Reinventing the Regulatory State*, 62 U Chi L Rev 1, 8 (1995) (while detailing the different approaches taken by the Reagan, H.W. Bush and Clinton presidencies, finding that "[t]he key task for those interested in regulatory performance is to find ways of simultaneously promoting economic and democratic goals").

[2] Roger W. Cobb and Charles D. Elder, *Participation in American Politics: The Dynamics of Agenda-Building* 164 (Johns Hopkins 2d ed 1983) (explaining that "mass participation may be one of the major innovative forces in developing new issues and refining old issues that have remained on the formal agenda for some time"); Stuart Langton, *Citizen Participation in America: Current Reflections on the State of the Art*, in Stuart Langton, ed, *Citizen Participation in America: Essays on the State of the Art* 7 (Lexington 1978) (explaining that "citizen participation has developed as an alternative means of monitoring government agencies"); Jerry L. Mashaw, *Due Process in the Administrative State* 169 (Yale 1985) (arguing that the dignitary model is both necessary and sufficient to structure a conversation about public values); Roger C. Cramton, *The Why, Where, and How of Broadened Public Participation in the Administrative Process*, 60 Georgetown L J 525 (1972) (arguing that broadened public participation improves the administrative decisionmaking process, giving decisions greater legitimacy and acceptance); Steven Kelman, *Adversary and Cooperationist Institutions for Conflict Resolution in Public Policymaking*, 11 J Pol Analysis & Mgmt 178, 180 (1992) (arguing that public participation allows for cooperationist institutions to solve problems among themselves).

nature of agency decisions.[3] Agencies' expertise is said to produce rational policies insulated from politics.[4]

Little attention has been paid to how information technologies might advance these efforts. To date, the main contribution of digital technologies is e-Rulemaking.[5] Yet e-Rulemaking does little more than re-package the twentieth-century approach to policymaking,[6] which itself has proven problematic.[7] This barely touches information technology's potential for improving the legitimacy of the administrative state.

Information systems offer that opportunity. Agencies increasingly transfer crucial responsibilities to computer systems. Computers gather and interpret important data. For example, electronic machines record and calculate votes. Information systems incorporate and apply policy, making decisions about important individual rights, such as a person's ability to receive public benefits.[8] And computers store sensitive information, in-

[3] See Lawrence Lessig and Cass R. Sunstein, *The President and the Administration*, 94 Colum L Rev 1 (1994) (arguing that the President should be the primary overseer of agencies within particular limits).

[4] See Charles E. Lindblom, *The Intelligence of Democracy: Decision Making Through Mutual Adjustment* 137–41 (Free Press 1965) (explaining how insulating decisionmakers from the need to consider all possible value judgments leads to more rational decisionmaking); Thomas O. McGarity, *Reinventing Rationality: The Role of Regulatory Analysis in the Federal Bureaucracy* 10 (Cambridge 1991) (explaining the essential elements of rational decisionmaking).

[5] The term e-Rulemaking refers to the use of digital technologies to enhance the public's understanding of, and participation in, agency notice-and-comment rulemaking. To that end, the federal government's Regulations.gov website allows the public to search, view, and comment on certain proposed rules. E-Gov Website, E-Rulemaking, available at <http://www.whitehouse.gov/omb/egov/c-3-1-er.html> (last visited Apr 24, 2008) (describing public launch of Regulations.gov website, a "cross agency front-end web application that posts and allows comments on proposed federal agency rules"). Some scholars have embraced e-Rulemaking efforts as a means to democratize agency policymaking. See Beth S. Noveck, *The Electronic Revolution in Rulemaking*, 53 Emory L J 433, 435–36 (2004) (discussing e-Rulemaking as a way to reform the administrative process).

[6] Stuart M. Benjamin, *Evaluating E-Rulemaking: Public Participation and Political Institutions*, 55 Duke L J 893, 897, 923–29 (2006) (arguing that proponents and skeptics of e-Rulemaking have not considered the role of the courts and Congress in the larger administrative law context and contending that e-Rulemaking efforts will exact high costs with little net benefit).

[7] See John M. Mendeloff, *The Dilemma of Toxic Substance Regulation: How Overregulation Causes Underregulation at OSHA* 7–16 (MIT 1988) (complaining that agencies skirt informal rulemaking process due to its cost by making policy in other ways); Jerry L. Mashaw & David L. Harfst, *Regulation and Legal Culture: The Case of Motor Vehicle Safety,* 4 Yale J Reg 257 (1987) (explaining how the cumbersome rulemaking process has caused the National Highway Traffic Safety Administration to abandon ambitious safety regulations in favor of a recall procedure).

[8] Danielle Keats Citron, *Technological Due Process*, 85 Wash U L Rev 1249, 1260–67 (2008).

cluding federal employees' personal data.[9] Because these systems profoundly affect the public, the ability to monitor them is essential to the administrative state's transparency, participatory nature, rationality, and hence its democratic legitimacy.

These systems, however, are opaque. Because these systems' software is proprietary, the source code—the programmers' instructions to the computer—is secret. Closed source code[10] leaves users unable to discern how a system operates and protects itself. Thus, users have difficulty detecting programming errors that disenfranchise voters[11] and undercount communities for the census. Programming mistakes that distort established policy routinely remain hidden from view.

These systems' opacity interferes with important administrative law values. Closed code prevents public participation in agency decisions incorporated in these systems. Unlike interested members of the public who have opportunities to collaborate in policymaking through comments on proposed rules, stakeholders cannot provide feedback on agency decisions that they cannot see.[12] At the same time, opaque systems impair the administrative state's political accountability.[13] The public cannot hold elected officials responsible for broken systems without opportunities to learn about these systems' problems. Closed sys-

---

[9] See, for example, Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S Cal L Rev 241, 248–49 (2007).

[10] Wikipedia, *Proprietary Software*, available at <http://en.wikipedia.org/wiki/Proprietary_software> (last visited Apr 24, 2008). Throughout this Article, I will refer to systems whose source code is closed to the public as "closed systems." I also will refer to closed source code as "closed code." The instructions that run computers actually constitute several layers of code. Aviel D. Rubin, *Brave New Ballot: The Battle to Safeguard Democracy in the Age of Electronic Voting* 3 (Morgan Road 2006). Source code provides the basic instructions to the computer. A program known as a compiler converts the source code into object code, a stream of ones and zeros comprehensible only to machines that runs inside the computer.

[11] Earl Barr, Matt Bishop, and Mark Gondree, *Fixing Federal E-Voting Standards*, Commun of the Assoc for Computing Machinery 19, 21 (Mar 2007) (arguing that open-code systems allow users to locate and repair flaws that would not be repaired under a closed system).

[12] See Lawrence Lessig, *Open Code and Open Societies*, in Joseph Feller, et al, eds, *Perspectives on Free and Open Source Software* 349, 358 (MIT 2005) (explaining that any law embedded in code is effectively "secret law").

[13] Frank Pasquale and Oren Bracha are engaged in an important enterprise regarding the opacity and lack of accountability in the operation of search engines. Oren Bracha and Frank A. Pasquale III, *Federal Search Commission?: Access, Fairness and Accountability in the Law of Search*, Cornell L Rev (forthcoming 2008); Frank A. Pasquale III, *Taking on the Known Unknowns*, Concurring Opinions (Aug 12, 2007), available at <http://www.concurringopinions.com/archives/2007/08/taking_on_the_k.html> (last visited Apr 24, 2008).

tems also undermine an agency's expertise by applying distorted policy and by closing off opportunities for the broader technical community to provide valuable feedback on systems' security and accuracy.

This Article proposes opening up these black boxes to improve the quality and democratic legitimacy of agencies' decisionmaking. My proposal would require vendors to release certain systems' source codes for public review. High profile systems, such as e-voting machines, would command the attention of a wide array of technical experts,[14] while other automated systems would likely be studied by affected interest groups.[15]

Thus, an open code[16] model could invigorate the participatory model of the administrative state. In recent years, the cost and delay of involving the public has tempered enthusiasm for participatory approaches to administrative law.[17] This proposal would secure valuable public input while reducing the cost of obtaining it.

This proposal should appeal to advocates of strong central executive leadership. Open code will allow politically accountable actors, such as presidents and governors, to oversee agencies more directly. By contrast, closed code leaves those officials dependent on junior subordinates for accounts of what agencies' automated systems are doing and why.

At the same time, the input of programmers advances administrative law's goal of marshalling expertise to improve governance. Going back to Judge Landis and Justice Frankfurter, judges and scholars have argued that rational policy is best

---

[14] See notes 174–83 and accompanying text discussing technical community's interest in reviewing source code of e-voting systems.

[15] See note 184 and accompanying text discussing stakeholders interested in automated systems.

[16] This Article uses the term "open code" to refer to software whose source code is available for public review. In using this term, I distinguish open code software from "open source software" or "free software," whose source code is similarly revealed to the public but also enjoys relaxed licensing terms. Lessig, *Open Code and Open Societies* at 358 (cited in note 12); Jesus M. Gonzalez-Barahona and Gregorio Robles, *Libre Software in Europe*, in Chris DiBona, Danese Cooper, and Mark Stone, eds, *Open Sources 2.0: The Continuing Evolution* 161 n 1 (O'Reilly 2006); L. Jean Camp, *Varieties of Software and their Implications for Effective Democratic Government*, 135 Proceedings of the British Academy 183 (2006), available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=905277> (last visited Apr 24, 2008). This Article leaves aside the question of the licensing regime that should govern such software, such as whether the software would be free to use, modify, or sell.

[17] See Jim Rossi, *Participation Run Amok: The Costs of Mass Participation for Deliberative Agency Decisionmaking*, 92 Nw U L Rev 173, 217–18 (1997) (explaining how increased participation greatly increases the costs of ordinary agency decisions).

achieved through expert scrutiny of difficult problems.[18] This model, however, depends on expert agencies having sufficient data to make optimal decisions.[19] Open code makes new programming and system design expertise relevant and available to the administrative state.[20]

This Article proceeds in three parts. Part I provides a typology of closed systems used by administrative agencies. It identifies two serious problems that closed systems conceal: programming errors that cause inaccurate results and security vulnerabilities that can lead to serious problems, such as identity theft and election fraud.

Part II articulates the contours of an open code model. It then lays the normative foundations for such a regime, exploring how open code advances critical administrative law values of participation, political accountability, and expertise.[21] Part II argues that this proposal favoring open code would render agency decision-making mechanisms embedded in these systems more transparent, participatory, and expert.

Part III discusses three potential objections to an open code model. First, will switching from closed systems to an open code model be unduly costly? This Article argues that short-term costs should be balanced against the long-term gains that transparency brings. Second, will only high profile systems, such as e-voting, generate feedback, leaving the rest of these systems unexamined? This Article answers this question in the negative and explains that openness will provide important benefits even if these systems are not actually reviewed. Third, does an open code regime compromise privacy and security? The computer security literature rejects a "security through obscurity" regime and underscores the importance of openness to identify security

---

[18] James M. Landis, *The Administrative Process* 6–46 (Yale 1938); Henry H. Perritt, Jr, *The Electronic Agency and the Traditional Paradigms of Administrative Law*, 44 Admin L Rev 79, 88–89 (1992).

[19] Stephen G. Breyer, *Active Liberty: Interpreting Our Democratic Constitution* 102–03 (Knopf 2005).

[20] Vladi Finotto and Angela Forte, *Re-Use of Solutions and Open Source Software in Public Administrations*, in Eleonora Di Maria and Stefano Micelli, eds, *On Line Citizenship: Emerging Technologies for European Cities* 140 (Springer 2005) ("By liaising with open source software developer communities, local public administrations can adopt a specific application and contribute to its evolution while enjoying the benefits of full access to a global pool of experts and developers ready to fix problems and suggest solutions.").

[21] Naturally, each of these models of administrative law has been subject to criticism. This Article does not address those debates but instead endeavors to show how the varying models of administrative law would support this proposal.

vulnerabilities. This Article concludes by offering some refinements to the proposal described in Part II.

I. CLOSED CODE IN THE ADMINISTRATIVE STATE

Information systems used by agencies bring important benefits to the administrative state. For instance, automated systems cut costs, allowing agencies to manage data efficiently,[22] and they apply policy in a uniform manner. This Part provides a typology of systems whose source code is closed and then explores the problems they raise.

A. Typology of Closed Systems

Agencies employ closed systems in one of three types.[23] The first type collects and processes information.[24] A prominent type of data processing system is electronic voting machines. After the passage of the Help America Vote Act in 2002,[25] municipalities, counties, and states rushed to buy electronic voting systems[26] that record and tally votes.[27] Private vendors build e-voting systems, incorporating both commercial off-the-shelf software and their own software.[28] Election Systems & Software ("ES&S"),

---

[22] William D. Eggers, *Government 2.0: Using Technology to Improve Education, Cut Red Tape, Reduce Gridlock, and Enhance Democracy* 29 (Rowman and Littlefield 2005).

[23] This Article does not endeavor to present an exhaustive taxonomy of information systems used by agencies. Instead, it categorizes information systems that have a profound effect on public policy and important individual rights and whose opacity impacts important administrative law values.

[24] This Article refers to such systems as "data processing systems."

[25] The Help America Vote Act of 2002 ("HAVA") established a program to "provide funds to States to replace punch card voting systems" with e-voting systems. Pub L No 107-252, 116 Stat 1666 (2002), codified at 42 USC §§ 15301–15545 (Supp 2004). HAVA authorized the annual release of over a billion dollars to fund state upgrades of voting equipment for fiscal years 2003–2005. 42 USC § 15407 (Supp 2004).

[26] This Article uses the terms "e-voting systems" and "e-voting machines" to refer to computerized systems that record in electronic form voters' selections. E-voting systems, of course, come in varying types, such as Direct Recording Electronic systems ("DREs") without paper trails, DREs with Voter-Verifiable Paper Trails, and Precinct Count Optical Scans. See Brennan Center for Justice, *The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost* 2–4 (Brennan Center 2006), available at <http://www.brennancenter.org/dynamic/subpages/download_file_38150.pdf> (last visited Apr 24, 2008).

[27] Rubin, *Brave New Ballot* at 13 (cited in note 10).

[28] Hearing Before the Subcommittee on Elections of the House Committee on House Administration, 110th Cong, 1st Sess 2 (Mar 15, 2007) (testimony of Professor David Wagner), available at <http://www.cs.berkeley.edu/~daw/papers/testimony-house07.pdf> (last visited Mar 6, 2008) (hereinafter Wagner Testimony) (stating that "a voting system vendor like Diebold might license software from Microsoft for use in their touchscreen voting machine"). Those vendors typically do not have permission to provide the source

Diebold, Sequoia, and Avante manufacture most of this country's e-voting systems.[29]

E-voting systems use proprietary software.[30] As a result, election officials, candidates, technical experts, and interested citizens typically cannot inspect the source code to ensure the software works correctly.[31] Courts provide trade secret protection to the source code, refusing access to it even in cases where programming errors allegedly caused election irregularities.[32]

Another data processing system is the Census Bureau's Current Population Survey ("CPS"). CPS uses Windows-based software that processes interviews and aggregates census data to determine the amount of federal aid distributed to state and local governments, including housing assistance, public benefits, and

---

code to others.

[29] See *The Machinery of Democracy* at 2–4 (cited in note 26) (cataloging manufacturers of various systems). More than 150,000 voting machines in use around the country are Diebold systems. Kim Zetter, *Diebold to Change Its Name*, Wired (Aug 16, 2007), available at <http://blog.wired.com/27bstroke6/2007/08/diebold-to-chan.html> (last visited Feb 24, 2008).

[30] Bev Harris, *Black Box Voting* 26 (Plan Nine 2004); Rubin, *Brave New Ballot* at 13 (cited in note 10).

[31] Wagner Testimony at 2 (cited in note 28). Because each state has its own election laws, voting equipment must meet state requirements and federal voting system guidelines, which have been adopted by most states. Lisa Vaas, *U.S. e-Voting Lags*, e-Week, 26 (Aug 13, 2007). Federal voting standards ask vendors to share their source code with a testing laboratory selected by the vendor. Id. Such voting systems testing laboratories must be accredited by the Election Assistance Commission. Id. Only fifteen states require manufacturers, in some manner, to place source code in escrow for examination. Verified Voting Foundation, *Escrow of Voting Software* (April 17, 2007), available at <http://www.verifiedvoting.org/downloads/EscrowProvisions.pdf> (last visited Apr 24, 2008).

[32] See *Christine Jennings v Elections Canvassing Commissionn of Florida*, 958 S2d 1083 (Fla App 2007) (denying petition for certiorari to review district court's refusal to compel discovery of e-voting machines' source code); Ryan Paul, *Court: Protecting Trade Secrets Takes Priority over Election Transparency*, Ars Technica (June 25, 2007), available at <http://arstechnica.com/news.ars/post/20070625-florida-appeals-court-says-trade-secret-protection-takes-priority-over-election-transparency.html> (last visited Feb 24, 2008).

unemployment.[33] Census 2000 affected the allocation of over two trillion dollars.[34]

The second type of automated system executes policy and renders decisions about individuals.[35] Programmers building these systems translate policy into code.[36] For example, automated public benefits systems suggest eligibility determinations and benefit calculations to case workers.[37] Similarly, the Internal Revenue Service uses a decision-making system that identifies individuals who should be subject to tax audits.[38]

The third type of closed system stores and disseminates sensitive information.[39] For instance, data storage systems collect contract data for the Department of Homeland Security.[40] State election boards maintain databases of eligible voters.[41] State and federal agencies store the sensitive personal information of em-

---

[33] Email from Fran Horvath, Office of Employment & Unemployment Statistics, Bureau of Labor Statistics, to Alice B. Johnson, Research Fellow, University of Maryland School of Law (Sept 20, 2007) (on file with the *University of Chicago Legal Forum*) ("Horvath Email"). The Current Population Survey ("CPS") is collected by the Census Bureau on behalf of the Bureau of Labor Statistics. Id. Once interviews are collected, closed code software known as Blaise processes the information. Id. The Bureau uses these products to aggregate micro data, which is seasonally adjusted. Id. Seasonal adjustments are made by a software program that is open code and available to the public for downloading. Id; US Census Bureau, *The X-12-ARIMA Seasonal Adjustment Program*, available at <http://www.census.gov/srd/www/x12a/> (last visited Feb 24, 2008); Kenneth Prewitt, *The US Decennial Census: Political Questions, Scientific Answers*, 26 Population & Dev Rev 1, 5–6 (2000).

[34] Prewitt, 26 Population and Dev Rev at 6 (cited in note 33). Given these stakes, it is "no surprise that there is a partisan edge to the focus on census numbers." US Government Accountability Office, Rep No GAO-06-567, *Federal Assistance: Illustrative Simulations of Using Statistical Population Estimates for Reallocating Certain Federal Funding* 3–4 (2006) (explaining that Census data determines federal grant programs such as Medicaid, Temporary Assistance for Needy Families, National School Lunch Program, Head Start, transit grants, child support enforcement, state administrative matching for food stamp program, public housing funds, and unemployment insurance).

[35] This Article refers to the second type of automated system as "decision-making systems."

[36] See Citron, 85 Wash U L Rev at 1260–61, 1281–88 (cited in note 8) (addressing the due process problems raised by decisionmaking systems).

[37] California, Colorado, Texas, and Florida employ such systems. See Terry Sapp, *Making Things Happen*, 64 Policy & Practice 40 (June 1, 2006) (discussing the use of public benefits system in California); Cynthia V. Fukami and Donald J. McCubbrey, *Colorado Benefits Management System (B): The Emperor's New System*, 18 Commun of the Assoc for Info Sys 488 (2006) (discussing the new benefits management system in Colorado).

[38] Camp, 135 Proceedings of the British Academy 183 (cited in note 16).

[39] This Article refers to the third type as "data storage systems."

[40] Ellen Nakashima and Brian Krebs, *Contractor Faulted in DHS Data Breach*, Wash Post A1 (Sept 24, 2007).

[41] Jennifer Granick, *Let Post-Election Debugging Begin*, Wired (Nov 8, 2006), available at <http://www.wired.com/politics/law/commentary/circuitcourt/2006/11/72083> (last visited Feb 24, 2008).

ployees and citizens.[42] The Environmental Protection Agency's data registry collects information about firms' environmentally-related activities that is then released in an annual report.[43]

B. Problems of Closed Systems

1. Inaccuracy.

Programming errors in closed systems frequently cause inaccurate findings.[44] Such errors are particularly common in data processing and decision-making systems. As this section explains, software errors can disenfranchise voters, undercount communities for the census, and distort policies in automated public benefits systems.

In hundreds of instances, e-voting machines have lost or added votes.[45] In November 2006, e-voting systems in Florida failed to record eighteen thousand ballots in a hotly contested congressional race.[46] During the 2006 primaries, e-voting machines in Cuyahoga County, Ohio made serious errors: "in 72.5

---

[42] See Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* 182 (NYU 2004); Citron, 80 S Cal L Rev at 295 (cited in note 9).

[43] Daniel J. Fiorino, *Rethinking Environmental Regulation: Perspectives on Law and Governance*, 23 Harv Envir L Rev 441, 448 (1999) (discussing federal Toxics Release Inventory). The EPA's data registry runs on Oracle's proprietary software. Telephone Interview by Alice B. Johnson with Nathan Wilkes, Environmental Protection Agency, Environmental Data Registry (Sept 28, 2007).

[44] To be sure, the programming errors and security problems discussed in this section occur in both open and closed systems. But these problems are particularly troubling in closed systems as they cannot be easily identified and fixed.

[45] Clive Thompson, *Can You Count on Voting Machines?*, NY Times Magazine 40 (Jan 6, 2008), available at <http://www.nytimes.com/2008/01/06/magazine/06Vote-t.html> (last visited Feb 24, 2008). See also Harris, *Black Box Voting* at 4–16 (cited in note 30); Rubin, *Brave New Ballot* at 61 (cited in note 10) (finding "gross design and programming errors" in Diebold machines); US Government Accountability Office, Rep No GAO 05-956, *Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed* 2 (2005); Barr, Bishop, and Gondree, *Fixing Federal E-Voting Standards* at 19 (cited in note 11); Donald P. Moynihan, *Building Secure Elections: E-Voting, Security, and Systems Theory*, 64 Pub Admin Rev 515, 519 (2004).

[46] Kim Zetter, *Academics Call Foul on Florida Test of Voting Machines*, Wired (Apr 16, 2007), available at <http://blog.wired.com/27bstroke6/2007/04/academics_call_.html> (last visited Feb 24, 2008). Just before the election, ES&S admitted that its poor software design risked losing votes. Kim Zetter, *Docs Point to E-Voting Bug in Contested Race*, Wired (Apr 17, 2007), available at <http://www.wired.com/politics/onlinerights/news/2007/04/evotinganalysis> (last visited Feb 24, 2008); Kim Zetter, *E-Vote Memo is a "Smoking Gun,"* Wired (Mar 22, 2007), available at <http://www.wired.com/politics/law/news/2007/03/EVOTE_0322> (last visited Feb 24, 2008); Kim Zetter, *Ohio Audit Says Diebold Vote Database May Have Been Corrupted*, Wired (Apr 19, 2007), available at <http://blog.wired.com/27bstroke6/2007/04/diebold_vote_da.html> (last visited Feb 24, 2008).

percent of the audited machines, the paper trail did not match the digital tally on the memory cards."[47]

In 2004, e-voting machines in an Ohio precinct recorded 3,893 votes for President Bush even though only 800 individuals were registered to vote there.[48] In Indiana, e-voting machines counted 144,000 votes in a county that only had 5,352 registered voters.[49] In 2002, Florida's e-voting machines lost as much as 21.5 percent of the votes in certain counties.[50] In 2000, e-voting machines in Iowa recorded four million votes when roughly three hundred ballots were inputted.[51]

Local officials caught these errors due to the obvious disparities between the number of votes cast and the number of registered voters.[52] In some cases, official inquiry into these errors led to the discovery of other problems, including a vendor's failure to certify[53] its e-voting machines.[54] But less obvious errors, such as switching votes from one candidate to another, are much more likely to go unnoticed.[55] A July 2007 investigative report re-

[47] Thompson, *Voting Machines*, NY Times Magazine (cited in note 45).

[48] John Schwartz, *Glitch Found in Ohio Counting*, NY Times A12 (Nov 6, 2004). In Franklin County, Ohio, an e-voting system reported that Bush received 4,258 votes against 260 for Kerry in a precinct where only 638 voters had cast ballots. Rubin, *Brave New Ballot* at 259 (cited in note 10).

[49] Cynthia L. Webb, *Cashing in on E-Voting?*, Technews.com (Financial Times Nov 13, 2003).

[50] Vaas, *US e-Voting Lags*, e-Week at 26 (cited in note 31). ES&S e-voting machines failed to count 103,222 votes in Broward County, Florida. *More Ballots Found in Florida; Outcome Same*, Omaha World-Herald 6a (Nov 9, 2002).

[51] Jim Carlton, Fuzzy Numbers: *Election Snafus Went Far Beyond Florida in Year When it Mattered*, Wall St J A1 (Nov 17, 2000).

[52] Moynihan, 64 Pub Admin Rev at 519 (cited in note 45).

[53] Certification provides independent verification that voting systems comply with the "functional capabilities, accessibility, and security requirements necessary to ensure the integrity and reliability of voting systems." Wikipedia, *Certification of Voting Machines*, available at <http://en.wikipedia.org/wiw/Certification_of_voting_machines> (last visited Feb 24, 2008). Under HAVA, the U.S. Election Assistance Commission ("EAC") bears responsibility for accrediting voting system test laboratories and certifying voting equipment through the Voting System Certification & Laboratory Accreditation Program. Id. Although federal certification for voting machines is voluntary, most states require such certification for their voting systems. See also note 31 discussing the EAC's role in accrediting e-voting systems.

[54] Kim Zetter, *ES&S to be Rebuked, Fined and Possibly Banned in CA?*, Wired, (Aug 21, 2007), available at <http://blog.wired.com/27bstroke6/2007/08/ess-to-be-rebuk.html> (last visited Feb 24, 2008) (reporting California's accusation that ES&S sold it machines that had not been tested or certified for use). The report also noted that ES&S assembled its machines in a sweatshop in the Philippines. Id. Due to problems with ES&S e-voting machines, Sarasota County in Florida committed to switching to Diebold machines in July 2007. Kim Zetter, *Florida County at Center of Election Storm Dumps ES&S in Favor of Diebold*, Wired (June 7, 2007), available at <http://blog.wired.com/27bstroke6/2007/06/florida_county_.html> (last visited Feb 24, 2008).

[55] Adam Cohen, *What's Wrong with My Voting Machine?* NY Times A24 (Dec 4, 2006)

vealed that 30 to 40 percent of ES&S's e-voting machines under review changed voters' selections.[56] Colorado's Secretary of State decertified e-voting systems manufactured by ES&S because tests demonstrated that the machines could not accurately count votes.[57]

Software flaws in e-voting machines raise concerns about the accuracy of other data processing systems. For instance, programming errors in CPS could result in inequitable funding for communities.[58] Software flaws that cause miscounts would deny local jurisdictions funds from federal programs.[59] If CPS undercounts the population in a jurisdiction with concentrations of groups requiring federal assistance, members of those groups will be deprived of entitlements that the benefits systems were designed to provide them.[60]

Decision-making systems are also riddled with programming flaws. When computer programmers translate policy into automated public benefits systems, they often distort it.[61] This is so

(noting reports of "vote flipping" in Broward County, Florida in November 2006 election); Todd R. Weiss, *'Vote Flipping' Is Real, but Its Cause Is the Subject of Debate*, Computerworld.com (Nov 13, 2006), available at <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=273455> (last visited Feb 24, 2008).

[56] Kim Zetter, *ES&S Discloses Full List of Manufacturers*, Wired (Aug 27, 2007), available at <http://blog.wired.com/27bstroke6/2007/08/ess-discloses-f.html> (last visited Feb 24, 2008). Further complicating matters is the fact that voter-verified paper trails are not required in twenty-three states. Ian Urbina and Christopher Drew, *Big Shift Seen in Voting Methods with Turn Back to a Paper Trail*, NY Times A1 (Dec 8, 2006) (explaining that e-voting machines used in Georgia and Maryland do not produce voter-verified paper trails). Without such paper trails, voters have no means to check if e-voting machines actually recorded their votes. Adam Cohen, *The Good News (Really) About Voting Machines*, NY Times (Jan 10, 2007); Steven Levy, *Black Box Voting Blues*, Newsweek 69 (Nov 3, 2003). But even when e-voting machines produce paper trails, nothing guarantees that the machines actually recorded the vote as cast or at all.

[57] *E-Vote: Colorado Tests Voting Equipment, Decertifies Some*, Government Technology (eRepublic Dec 18, 2007), available at <http://www.govtech.com/gt/articles/237095?utm_source=newsletter&utm_medium=email&utm_campaign=GTEN%20-%20E-Newsletter_2007_12_19> (last visited Feb 24, 2008).

[58] Prewitt, 26 Population & Dev Rev at 7 (cited in note 33).

[59] Id at 8.

[60] Id.

[61] Pamela Martineau, *With Lessons Learned, Yolo Launches CalWIN Program*, Sacramento Bee B1 (May 3, 2005) (noting pay discrepancies to welfare and general assistance recipients due to programming errors); Evelyn Larrubia and Caitlin Liu, *County's Computer System is Botching Medical Benefits Aid*, LA Times H1 (Feb 17, 2002) (explaining that computer errors resulted in denial of prenatal care); *Tamara Clark v Department of Children & Family Services*, No 05-2105RP, *Petition to Determine Invalidity of Proposed Rule 65A-1.400 and ESS Online Benefits Application Form* 6 (Fla Div Admin Hearings June 10, 2005) (arguing that relative caregivers could not apply for Temporary Assistance to Needy Families due to the design of the online application in violation of Florida law).

for several reasons. Although all translations shade meaning,[62] a translation of policy from human language into code poses a more significant risk of radically altering that policy than would a translation from English to another human language.[63] This is in part because artificial languages intelligible to computers have a limited range of key words as compared to human languages.[64] Computer languages thus may be unable to capture a policy's nuances.[65]

Code writers interpret policy when they translate it from human language to computer language.[66] Distortions in policy have been attributed to the fact that programmers building code lack "policy knowledge."[67] This is neither surprising nor easily remedied. Private information technology consultants cannot be expected to have specialized expertise in regulatory or public benefits programs. And programmers working for government agencies tend to work on a wide variety of programs, preventing them from developing expertise in any given area.

Policy changes may stem from a programmer's values.[68] Programmers can unconsciously phrase a question in a biased manner.[69] In a complex software system composed of smaller subsys-

---

[62] See generally Jacques Derrida, *Of Grammatology* (Johns Hopkins 1976) (Gayatri Chakravorty Spivak trans); see also J.M. Balkin, *Deconstructive Practice and Legal Theory*, 96 Yale L J 743, 783–86 (1987).

[63] Australian Administrative Review Council, *Automated Assistance in Administrative Decision Making* 18 (2004), available at <http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(E671321254BE241EF50E9203E76822F1)~AAADMreportPDF.PDF> (last visited Feb 24, 2008) (hereinafter Aus Admin Rev, *Automated Assistance*).

[64] Id; James Grimmelmann, Note, *Regulation by Software*, 114 Yale L J 1719, 1728 (2005).

[65] Graham Greenleaf, Andrew Mowbray, and Peter van Dijk, *Representing and Using Legal Knowledge in Integrated Decision Support Systems: DataLex WorkStations*, 3 Artificial Intelligence & L 97, 127 (1995).

[66] Aus Admin Rev, *Automated Assistance* at 29 (cited in note 63).

[67] Office of Inspector General, Texas Health & Human Services Comm, *TIERS/IEES Review* 29 (2007) (copy on file with U Chi Legal F); Deloitte, *State of Colorado: CBMS Post-Implementation Review* 9 (May 2005) (copy on file with U Chi Legal F) (explaining that incorrect rules embedded in CBMS were in part due to incorrect policy interpretation by programmers). But see Jessica Weidling, *Housing Hopes* 47, Government Tech (June 2007) (noting that in "uncharacteristic move for the public sector," Philadelphia Housing Authority administrators spent time with software provider to carefully discuss requirements of their automated telephone system).

[68] Code embeds the values and choices of the code writer. Lawrence Lessig, *Code Version 2.0* 102 (Basic 2006).

[69] See Helen Nissenbaum, *How Computer Systems Embody Values*, Computer 119 (Mar 2001) (explaining that systems can unfairly discriminate against specific sectors of users); Batya Friedman and Helen Nissenbaum, *Bias in Computer Systems*, 14 Assoc Computing Machinery Transactions on Info Systems 330, 333 (1996) (describing automated loan program whose system assigns negative value to applicants from certain locations, such as high-crime or low-income neighborhoods).

tems, the actual bias of the system "may well be a composite of rules specified by different programmers."[70]

Inaccuracy can spring from a code writer's preference for binary questions that are easily translated into code.[71] Policy, however, often involves the weighing of multiple variables.[72] There is a significant risk that code writers may fail to accurately capture these nuances given their bias for binary choices.[73] Programmers also may inappropriately narrow the discretion available to a system's users.[74]

Distorted policy might also stem from an agency's decision to automate policy changes that require, but have not received, rulemaking procedures. Professor Evelyn Brodkin has studied frontline bureaucratic routines that create new policy at the point of delivery.[75] For instance, lower-level bureaucrats often make policy when established policy is internally contradictory.[76] Such practices produce "street-level" welfare policies that have not been published and vetted through notice-and-comment rulemaking procedures.[77] Decision-making systems could automate such policy.[78]

Whether distorted policy stems from programming errors or deliberate agency action, the resulting inaccuracy is the same. Automated public benefits systems in California, Colorado, Florida, and Texas incorporated distorted policies that changed es-

---

[70] Grimmelmann, 114 Yale L J at 1737 (cited in note 64).

[71] Denise Kersten, *Bytes vs. Brains*, 37 Government Exec 30 (Sept 1, 2005) (explaining the difficulties that may arise from translating more complex inquiries into code).

[72] For example, the Food Stamp Act and federal regulations limit food stamps of childless adults to three months with six exceptions, which cross reference other exceptions that, in turn, refer to still other exceptions. 7 USC § 2015(o) (2000); 7 CFR § 273.25 (2008). Those writing code may be tempted to impose a three-month rule without the complicated and arguably confusing exceptions. See David A. Super, *Are Rights Efficient? Challenging the Managerial Critique of Individual Rights*, 93 Cal L Rev 1051, 1096 n 205 (2005) (discussing potential for eligible workers and those designing notices to read three-month rule with regard to childless adults seeking food stamps without regard to the exceptions).

[73] Aus Admin Rev, *Automated Assistance* at 21 (cited in note 63) (stating specific instances in which allowing an agency officer to override an expert system would be preferable).

[74] Id.

[75] Evelyn Z. Brodkin, *Street-Level Research: Policy at the Front Lines*, in Mary Clare Lennon and Thomas Corbett, eds, *Policy into Action: Implementation Research and Welfare Reform* 145 (Urban Institute 2003). Brodkin's important research aims to render this opaque policy more transparent.

[76] Id at 149.

[77] Id.

[78] Automated street-level welfare policy would require notice-and-comment rulemaking to the same extent that non-automated street-level policy would.

tablished rules, often in violation of federal and state law. For instance, code writers embedded over nine hundred incorrect rules into Colorado's Benefits Management System ("CBMS") from September 2004 to April 2007.[79] With one such incorrect rule, CBMS denied Medicaid to breast and cervical cancer patients based on income and asset limits that were not authorized by federal or state law.[80] Another distorted rule caused CBMS to discontinue food stamps to individuals with past drug problems in violation of Colorado law.[81] In all, CBMS rendered hundreds of thousands of erroneous eligibility decisions and benefits calculations.[82]

2. Security problems.

Data processing systems can have serious security problems. In 2007, California's Secretary of State launched an investigation of the state's e-voting systems.[83] Teams of computer scientists found "deep architectural flaws" in the source code of the state's e-voting machines.[84] These flaws rendered the e-voting systems

[79] See Colorado Benefits Management System, *Decision Table Release Notes Covering 2004–2007*; Deloitte, *CBMS Post-Implementation Review* at 10 (cited in note 67) (explaining that there were 175 distinct defects in the Medicaid rules table in 2005). For other incorrect rules encoded in the system, see Colorado Benefits Management System, *Decision Table Release Notes for February 24–25, 2007* 19 (Feb 26, 2007) (issuing correction of code that exempted a child's earnings in calculating food stamps where the child was the head of the household in contravention of federal regulations); Colorado Benefits Management System, *Decision Table Release Notes for August 12–13, 2006* 10 (Aug 11, 2006) (correcting embedded rule that did not allow Medicare premium as an expense for disabled individual in contravention of federal regulations).

[80] Colorado Benefits Management System, *Decision Table Release Notes for March 10–11, 2007* 10 (Mar 7, 2007) (fixing rule that improperly imposed income limits on women with breast or cervical cancer in violation of 42 USC § 1396r-1b and Colo Rev Stat Ann § 25.5-5-308).

[81] Colorado Benefits Management System, *Decision Table Release Notes for February 3–4, 2007* 24 (Feb 1, 2007) (correcting rule embedded in system that contravened Colo Rev Stat § 26-2-305, which mandates that individuals "shall not be ineligible [for food stamps] due to a drug conviction unless misuse of food stamp benefits is part of the court findings").

[82] David Migoya, *Feds Give Colorado a Big Bill*, Denver Post B1 (Apr 12, 2007) (explaining that CBMS made up to 11,000 errors per month).

[83] Joseph A. Calandrino, et al, *Source Code Review of the Diebold Voting System* (July 20, 2007), available at <http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf> (last visited Feb 24, 2008); Matt Blaze, et al, *Source Code Review of the Sequoia Voting System* (July 20, 2007), available at <http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia-source-public-jul26.pdf> (last visited Feb 24, 2008). California could order a review of the source code because it is one of the few states that mandate submission of the source code into escrow for official review.

[84] Calandrino et al, *Source Code Review* at 10–24 (cited in note 83). The voting machines subject to review were manufactured by Diebold Election Systems, Hart InterCivic, Sequoia Voting Systems, and Elections Systems and Software, Inc. Website of

vulnerable to attacks and bugs.[85] For instance, the source codes allowed the insertion of malicious code and viruses that would alter votes.[86]

Reviewers also found the source codes to be too complex to resist bugs.[87] One vendor incorporated Microsoft's Windows, which is notorious for security problems, in its system.[88] All of the state's e-voting systems used vulnerable encryption schemes, often with critical security codes stored in files as plain text.[89] Based on these findings, California's Secretary of State ordered vendors to fix the systems and has conditionally recertified them pending further review.[90] In December 2007, Colorado's Secretary of State decertified the state's Sequoia e-voting machines due to a variety of security risk factors.[91]

California Secretary of State Debra Bowen, *Top-to-Bottom Review*, available at <http://www.sos.ca.gov/elections/elections_vsr.htm> (last visited Feb 24, 2008). In 2003, computer scientists detected these same flaws when Diebold's source code was leaked onto the Internet. Kim Zetter, *CA Releases Source Code Review of Voting Machines—New Security Flaws Revealed; Old Ones Were Never Fixed*, Wired (Aug 3, 2007), available at <http://blog.wired.com/27bstroke6/2007/08/ca-releases-sou.html> (last visited Jan 23, 2008); Moynihan, 64 Pub Admin Rev at 520 (cited in note 45). See also text accompanying notes 125–26 (discussing the communities that uncovered and publicized the flaws in Diebold's e-voting machines in 2003).

[85] Wagner Testimony at 2 (cited in note 28) (describing the inadequacy of testing laboratories in finding security flaws); Calandrino, et al, *Source Code Review* at 10–24 (cited in note 83); IDG News Service, *Group Says e-Voting Paper Trail Wouldn't Improve Security*, Computerworld (Sept 18, 2007), available at <http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=it_in_government&articleId=9037399&taxonomyId=69&intsrc=kc_top> (last visited Feb 24, 2008); Vaas, *U.S. e-Voting Lags*, e-Week at 23 (cited in note 31). In 2006, computer scientist Professor Edward Felten analyzed an anonymously donated AccuVote-TS e-voting machine and discovered that the machine did not "authenticate" software—it would run any code a hacker would install on an easily inserted flash-memory card. Thompson, *Voting Machines*, NY Times Magazine (cited in note 45).

[86] Calandrino et al, *Source Code Review* at 10–24 (cited in note 83). One of the reports explained that creating a voting machine virus would require moderate programming skills and access to voting equipment, both of which are available. Id. Indeed, a Diebold system was recently listed on eBay. Id.

[87] Id at 24. Diebold's systems also used C and C++ programming languages, which are known to be prone to security problems. Id at 28–29.

[88] Id.

[89] Kim Zetter, *Help Feds Build a Better Voting Machine*, Wired (Sept 6, 2007), available at <http://blog.wired.com/27bstroke6/2007/09/tell-uncle-sam-.html> (last visited Feb 24, 2008). Quite alarmingly, San Diego County named a former sales representative for Diebold as its Registrar of voters. Kim Zetter, *Former Diebold Sales Rep Becomes Registrar of Voters in San Diego*, Wired (May 11, 2007), available at <http://blog.wired.com/27bstroke6/2007/05/former_diebold_.html> (last visited Feb 24, 2008).

[90] Robert McMillan, *California Puts Limits on Use of E-Voting Systems*, Computerworld (Aug 13, 2007), available at <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=300571> (last visited Feb 24, 2008).

[91] *E-Vote: Colorado Tests Voting Equipment*, Government Technology (cited in note 57).

Data storage systems also lack adequate security, facilitating the release of sensitive personal information kept by agencies. Consider these data leaks from 2006 and 2007. Attackers broke into the Department of Energy's computer system and stole Social Security numbers of federal employees.[92] Hackers breached the Nebraska Treasurer's system, stealing Social Security numbers and tax identification numbers from nine thousand businesses.[93] The Chicago Voter Database was breached, compromising the Social Security numbers of 1.35 million residents.[94] Attackers invaded the online database of Iowa's Department of Education, exposing sensitive personal data of six hundred individuals.[95] The release of sensitive personal data raises the risk of identity theft and stalking.[96]

Current legal mechanisms have not sufficiently addressed the security problems that afflict data storage systems. The E-Government Act of 2002[97] ("E-Government Act") requires federal administrative agencies to conduct privacy impact assessments ("PIAs") when developing or purchasing systems that collect, store, or disseminate personally identifiable information.[98] Pursuant to Office of Management and Budget ("OMB") guidance, PIAs must identify and evaluate potential threats to privacy, discuss alternatives, identify appropriate risk mitigation measures, and articulate the rationale for the final design choice.[99]

The E-Government Act, however, has achieved mixed results to date.[100] The incidence of agency noncompliance is significant: 12 percent of agencies do not have written processes or policies

---

[92] Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, available at <http://www.privacyrights.org/ar/ChronDataBreaches.htm> (last visited Feb 24, 2008).

[93] Id.

[94] Id.

[95] Id. For instance, independent contractor Unisys Corporation built and managed the information technology networks for the Transportation Security Administration and the DHS headquarters. Nakashima and Krebs, *Contractor Faulted*, Wash Post (cited in note 40). The closed nature of the system prevented the agency and the public from overseeing the system, which was subject to three months of cyber-intrusions by hackers. It allowed Unisys to falsely certify that the network had been protected to cover up its lax oversight. Id.

[96] Citron, 80 S Cal L Rev at 251–52 (cited in note 9).

[97] Pub L No 107-347, 116 Stat 2899.

[98] 44 USC § 3501 note (2000 & Supp 2002).

[99] See Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, M-03-22 (Sept 26, 2003),* available at http://www.whitehouse.gov/omb/memoranda/m03-22.html (visited June 16, 2008).

[100] Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U Chi L Rev 75, 76, 81–82, 83 (2008) (arguing that PIA process requirement is insufficient to address privacy concerns).

for all listed aspects of PIAs and 16 percent of systems covered by the PIA requirement did not have a complete or current PIA.[101] As Kenneth Bamberger and Deirdre Mulligan have forcefully argued, the E-Government Act may have little chance of future success in part due to the public's inability to comment on the design of systems whose specifications and source codes remain obscured.[102] An open code solution would tackle this problem.

The next Part suggests opening up these systems and explores why administrative law values support this proposal.

II. ENHANCING THE DEMOCRATIC AND EXPERT NATURE OF ADMINISTRATIVE GOVERNANCE WITH OPEN CODE

Closed code inhibits public participation in the development of critical information systems. Because the technical community has no opportunity to identify a system's problems, an uninformed public cannot press politically accountable actors to remedy them. With closed code, the expertise of a broader technical community is unavailable to agencies.

An open code model has the potential to redress these problems. This Part begins by developing that model. Then, it demonstrates how open code governance can advance the transparency, democratic legitimacy, and expertise of the administrative state.

A. Open Code Proposal

The source code of critical information systems should be open to the public.[103] Open code would reveal how a system works, shedding light on the policies encoded in it.[104] It would allow interested parties to discuss the assumptions that underlie

---

[101] Id at 81.

[102] Id at 88–89.

[103] See, for example, Lawrence Lessig, *The Limits in Open Code: Regulatory Standards and the Future of the Net*, 14 Berkeley Tech L J 759, 764 (1999) (arguing that open code decreases the opportunity for government regulation of code).

[104] David M. Berry and Giles Moss, *Free and Open-Source Software: Opening and Democratising e-Government's Black Box*, 11 Info Polity 21, 23 (2006) (discussing the benefits of non-proprietary software). Software architect Jon Garfunkel suggests that open business rules could run on top of a proprietary rules engine that constitutes the system's logic. Email from Jon Garfunkel, Senior Process Architect, Pegasystems, to Danielle Keats Citron (Dec 20, 2007) (copy on file with author and U Chi Legal F).

the digital processes.[105] And open code would permit inspection of a system's security features.[106]

This proposal does not insist that agencies eliminate private vendors and generate the code themselves, either by relying on volunteer programmers or on government information technology departments. Instead, vendors constructing these systems would be required to release the source code to the public before their purchase or implementation. Just as procurement contracts insist that government contractors refrain from discriminatory practices, agencies could require that vendors make transparent the source code for critical systems to facilitate public feedback and executive oversight. Computer security expert Bruce Schneier explains that systems built by private vendors whose source codes are opened to the public offer both safety and reliability.[107]

An open code model could be pursued in various ways. Agencies could insist on open code systems. Vendors would be required to release to the public a system's specifications and source code during the bidding process and before a purchased system goes live.[108] To that end, the OMB could issue a circular conditioning the provision of federal funding for technology purchases on the use of open code.[109] A state budget office could do the same for local purchases receiving state aid.

For example, the San Francisco Elections Commission ("Commission") has issued a non-binding appeal to California's Department of Elections to "make reasonable efforts to select and

---

[105] Camp, 135 Proceedings of the British Academy (cited in note 16). Programmers should provide comments that explain why they wrote the code they way that they did and exactly how they did it. See Posting of Rebecca Buckman, *Men Write Code From Mars, Women Write More Helpful Code From Venus*, Wall St J Blog (June 6, 2008), available at <http://blogs.wsj.com/biztech/2008/06/06/men-write-code-from-mars-women-write-more-helpful-code-from-venus/> (last visited June 30, 2008). The code would then become a roadmap for others who want to understand the policies embedded in it. Id. Emma McGrattan, one of Silicon Valley's highest-ranking programmers, has instituted new coding standards at Ingres, where she is a senior vice-president of engineering, which requires programmers to include a detailed set of comments before each block of code explaining what the piece of code does and why and a detailed history of any changes programmers make to the code. Id. I thank James Grimmelmann for this helpful point.

[106] Wagner Testimony at 3 (cited in note 28).

[107] Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* 344 (Wiley 2004).

[108] But see Yochai Benkler, *Freedom in the Commons: Towards a Political Economy of Information*, 52 Duke L J 1245, 1275 (2003) (advocating that software written for government should be released as "free software" under relaxed licensing regime to enhance the commons approach of software development).

[109] I thank my colleague David Super for this insight.

use voting systems technology, including hardware and software that at a minimum is publicly disclosed."[110] The Commission defined "public disclosure" as the right to inspect, test, and comment on technology during the procurement process.[111] Thus, if adopted, this policy would require prospective vendors to release their source codes during the bidding process.

Alternatively, legislators could mandate open code systems.[112] For instance, eighteen countries require the use of open source software in government offices.[113] In 2006, the California legislature held hearings on whether its electoral system should use open source software.[114] The next sections provide normative support for the use of open code software, relying on different models of the administrative state.

B. Participation Enhanced

Open code systems secure meaningful opportunities for public input, advancing the participatory model of administrative law. This model promotes collaboration between the public and agencies in setting and achieving policy goals.[115] Although the value of public participation varies depending on the context, it is viewed as generating better information for agency delibera-

---

[110] San Francisco Elections Commission, *Motions and Resolutions Passed by the San Francisco Elections Commission in 2007*, available at <http://www.ci.sf.ca.us/site/electionscommission_index.asp?id=55693> (last visited Feb 24, 2008).

[111] Id.

[112] See Jyh-An Lee, *New Perspectives on Public Goods Production: Policy Implications of Open Source Software*, 9 Vand J of Enter & Tech L 45, 61 (2006) (explaining that Germany, Spain, and the Netherlands have all passed resolutions urging their governments to use open-source software).

[113] Id at 60 (explaining that national legislatures of Belgium, Brazil, Bulgaria, Chile, Colombia, Costa Rica, France, Italy, Peru, Spain, and Ukraine require use of open-source software in government offices).

[114] Wayne Hanson, *California Holds Hearing on Open Source Software in Election Systems*, Government Tech (eRepublic Feb 8, 2006), available at <http://www.govtech.com/gt/articles/98361> (last visited Feb 24, 2008).

[115] This Article uses the term "participatory model" to refer to a constellation of theories of regulatory governance that envision regulation as the product of collective deliberation about regulatory goals and priorities. See, for example, Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 Minn L Rev 342, 377 (2004); Steven P. Croley, *Theories of Regulation: Incorporating the Administrative Process*, 98 Colum L Rev 1, 76 (1998). See also Cass R. Sunstein, *After the Rights Revolution: Reconceiving the Regulatory State* (Harvard 1990) (viewing governmental process as deliberation oriented to public good rather than series of interest-group tradeoffs); Gerald E. Frug, *Administrative Democracy*, in David H. Rosenbloom and Richard D. Schwartz, eds, *Handbook of Regulation and Administrative Law* 519, 520 (Marcel Dekker 1994).

tion.[116] This model envisions participation as enhancing an agency's legitimacy by cultivating the public's sense that it is involved in, and bears responsibility for, government.[117] In addition, participation is understood as offsetting the influence of well-organized interest groups through the inclusion of traditionally unrepresented interests.[118]

An open code model creates new opportunities for diverse groups to participate in the automated administrative state.[119] Networked technologies certainly make public participation easier and cheaper.[120] Digital networks facilitate peer production, a process by which individuals, whose actions are not coordinated either by managers or by market price signals, jointly produce information.[121] Peer production facilitates collaboration among "radically diverse" groups.[122] According to Yochai Benkler's social production theory, our networked information environment has produced a popular culture that encourages active participation

---

[116] Cass R. Sunstein, *Infotopia: How Many Minds Produce Knowledge* ix–x (Oxford 2006) (noting the author's experience with public participation via blogs); Jerry L. Mashaw, *Bureaucratic Justice: Managing Social Security Disability Claims* 140 (Yale 1983) (explaining the ways in which participation and control could contribute to claimants' sense of fairness); Benjamin R. Barber, *Strong Democracy: Participatory Politics for a New Age* 258–59 (Cal 1984) (explaining the problem of uncertainty in politics and noting that strong democratic politics encourages public participation); Cass R. Sunstein, *Factions, Self-Interest, and the APA: Four Lessons Since 1946*, 72 Va L Rev 271, 272, 282 (1986) (explaining the possible risks of factional tyranny and self-interested representation to the administrative process, particularly in light of the insulation of administrators from electoral control); Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 Harv L Rev 1285 (2003) (arguing that privatization may provide a way for traditionally public goals to be reached); Martha Minow, *Public and Private Partnerships: Accounting for the New Religion*, 116 Harv L Rev 1229, 1243 (2003) (arguing that favoring privatization increases competition, which creates pressure to generate information that may aid in administrative decisionmaking).

[117] Richard B. Stewart, *The Reformation of American Administrative Law*, 88 Harv L Rev 1669, 1709 (1975).

[118] Rossi, 92 Nw U L Rev at 211 (cited in note 17).

[119] See Russell J. Dalton, *The Good Citizen: How a Younger Generation is Reshaping Politics* 170 (CQ 2008) (explaining that younger Americans, such as members of Generation X and the Millennials, seem likely to seize upon new, networked opportunities for public participation). Political science research reveals that newer generations tend to connect with government through online public interest groups and internet discussion forums. Id at 75. This proposal would tap into these peer-to-peer networks and enhance the legitimacy of the administrative state.

[120] See Jonathan Zittrain, *The Future of the Internet—And How to Stop It* 92 (Yale 2008) (explaining that the generative Internet and PC make political and artistic expression easier).

[121] Benkler, 52 Duke L J at 1256 (cited in note 108).

[122] Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* 232 (Yale 2006). See Brett M. Frischmann, *Cultural Environment and The Wealth of Networks*, 74 U Chi L Rev 1083 (2007), for a thoughtful review of Yochai Benkler's *The Wealth of Networks*.

in matters of public policy.[123] Such "commons-based" participation arguably deepens the legitimacy of government action.[124]

Consider the online communities that exposed an e-voting system's flaws in 2003. Early that year, activist Bev Harris found Diebold's source code on the company's website.[125] Harris posted the source code on her website, urging viewers to examine and distribute it to file-sharing networks.[126] Internet discussion forums avidly discussed the source code's technical imperfections.[127] Computer scientists from Johns Hopkins and Rice University reviewed the source code, posting their criticism on the internet.[128]

A few months later, a hacker sent Harris a cache of internal Diebold emails that demonstrated the company knew that certain of its e-voting systems had problems.[129] After Harris posted the emails on her website, college students widely distributed them to peer-to-peer networks to keep the issue before the public.[130] In late 2003, California's Voting Systems Panel ("Panel") launched an investigation into Diebold's e-voting machines.[131] The Panel subsequently removed certain of the company's e-voting machines from the state's voting precincts.[132]

As the Diebold example suggests, revealing the source codes to the public would allow individuals and groups to study the accuracy and security of these systems.[133] For example, online

---

123 Benkler, *The Wealth of Networks* at 232 (cited in note 122).

124 Id.

125 Rubin, *Brave New Ballot* at 32 (cited in note 10).

126 Benkler, *The Wealth of Networks* at 232 (cited in note 122).

127 Harris, *Black Box Voting* at 104, 140–47 (cited in note 30).

128 Benkler, *The Wealth of Networks* at 227 (cited in note122). See Rubin, *Brave New Ballot* (cited in note 10) (describing his role in exposing weaknesses in Diebold source that Bev Harris discovered). Computer scientists found that a hacker could program a voter card to let it cast as many votes as the hacker liked. Thompson, *Voting Machines*, NY Times Magazine (cited in note 45).

129 Benkler, *The Wealth of Networks* at 227 (cited in note 122).

130 Id at 230.

131 Id.

132 Id at 231.

133 Berry and Moss, 11 Info Polity at 21 (cited in note 104); Andrew Chadwick, *Bringing E-Democracy Back in: Why It Matters for Future Research on E-Governance*, 21 Soc Sci Computer Rev 443, 452 (2003); Wagner Testimony at 4 (cited in note 28); Douglas W. Jones, *Voting System Transparency and Security: The Need for Standard Models*, Testimony before the Election Assistance Commission Technical Guidelines Development Committee, National Institute of Standards and Technology (Sept 20, 2004), available at <http://www.cs.uiowa.edu/~jones/voting/nist2004.shtml> (last visited Feb 24, 2008); Joseph Lorenzo Hall, *Transparency and Access to Source Code in E-Voting* (Berkeley Working Paper, 2006), available at <http://ssrn.com/abstract=909582> (last visited Feb 24, 2008).

communities could evaluate a system's design for hidden biases.[134] Programmers recruited by public interest groups could check the policies embedded in automated decision-making systems like CBMS. They could provide feedback on the privacy and security risks posed by proposed systems.[135]

This feedback would exert pressure on agencies to fix problems at the margins that they might be inclined to ignore. Such participation could enhance the public's perception of these systems.[136] Indeed, the Netherlands has focused its e-Government initiative on the adoption of open source software for the accuracy and legitimacy it brings.[137]

The public's participation could potentially combat interest-group capture of agencies and cronyism.[138] Open code could illuminate agency decisions that advance the interests of powerful groups.[139] For instance, if California's Department of Elections insists that vendors disclose their source codes during the bidding process, the technical community would have the opportunity to expose flaws in e-voting systems before election boards sign procurement contracts.[140] Such feedback might inhibit an

---

[134] Lessig, *Code Version 2.0* at 102 (cited in note 68) (arguing that members of the technical community now have power to restructure norms); Nissenbaum, *How Computer Systems Embody Values*, Computer at 119 (cited in note 69) (noting that engineers now face the challenge of building systems with certain moral properties).

[135] See Bamberger and Mulligan, 75 U Chi L Rev at 89 (cited in note 100) (explaining that because the PIA and other public documentation of e-Passport program did not provide the exact specifications of the system under consideration, the public could not review and test the proposed system). Professors Bamberger and Mulligan explain that the E-Government Act lacks explicit mechanisms for public participation in the PIA process, thus limiting opportunities for outside experts to assist the agency in identifying the privacy implications of complex data storage systems. Id. at 87. Although no formal process for public participation is provided under the E-Government Act, this proposal would enable outside groups and technicians to provide agencies with informal feedback on the security features and privacy problems posed by proposed systems.

[136] Berry and Moss, 11 Info Polity at 27 (cited in note 104). But see A. Michael Froomkin, *Technologies for Democracy*, in Peter M. Shane, ed, *Democracy Online: The Prospects for Political Renewal Through the Internet* 15 (Routledge 2004) (describing initiatives in England and Scotland that allow citizens to propose legislation via government website).

[137] OSOSS Webpage, available at <http://www.ososs.nl/about_ososs> (last visited Feb 24, 2008).

[138] The central concern here is that well-organized groups exercise disproportionate influence over agency policymaking. Stewart, 88 Harv L Rev at 1684–1687 (cited in note 117). Scholars have argued that administrative law ought to promote deliberative rationality and to constrain the influence of special interest groups. Sunstein, 72 Va L Rev at 271–96 (cited in note 116).

[139] Public choice theory contends that administrative regulation is little more than private contracts that benefit interest groups at the public expense. Jerry L. Mashaw, *Greed, Chaos, and Governance: Using Public Choice to Improve Public Law* 23–29 (Yale 1997).

[140] See text accompanying notes 104–05 discussing San Francisco Elections Commis-

agency's inclination to pick vendors based on political connections.[141] Open code thus has the potential to address concerns that special interests might dominate the procurement process.[142]

The drafters of the Administrative Procedure Act aimed to establish a system in which "citizens and representatives, operating through responsive but expert organs, would make deliberative decisions."[143] Scholars lament that these democratic aspirations have not been realized.[144] Public participation has withered in part due to the complexity of regulatory issues, the power of interest groups, and the expense of participation.[145]

Closed systems make this problem worse. Open code, however, could reverse this trend. It could also facilitate the participation of individuals who previously had little connection with the administrative state. As the next section discusses, informed citizens could pressure elected officials to ensure the accuracy

---

sion's recommendation that the state open up source code during procurement process.

[141] I thank my colleague Rena Steinzor for this insight. Activists have similar concerns about the impartiality of the companies that certify e-voting systems because vendors pay for their services and because their certification reports are not public. Barr, Bishop, and Gondree, *Fixing Federal E-Voting Standards*, Commun of the Assoc for Computing Machinery at 19 (cited in note 11). With few vendors selling e-voting machines, if one certification firm is too demanding, it would lose a huge share of its business if the vendor it criticized stops contracting with it. Indeed, it may be excluded from the industry if other vendors follow suit. Concerns about the impartiality of CIBER, which has certified most of this country's e-voting machines, were recently raised to the Federal Elections Assistance Commission. Kim Zetter, *New York to Grill Voting Machine Testing Lab*, Wired (May 4, 2007), available at <http://blog.wired.com/27bstroke6/2007/05/new_york_to_gri.html> (last visited Feb 24, 2008). CIBER lost its accreditation to certify voting machines in January 2007 due to its lax oversight of vendors' e-voting systems. Christopher Drew, *Citing Problems, U.S. Bars Lab from Testing Electronic Voting*, NY Times A1 (Jan 4, 2007). CIBER had been criticized for missing security and reliability problems long before its suspension. Id. See also Douglas W. Jones, *Misassessment of Security in Computer-Based Election Systems*, Cryptobytes at 9 (Fall 2004).

[142] Samir Chopra and Scott Dexter argue that the opacity of e-voting systems' design is a "secret compact between governments and manufacturers . . ., who alone are privy to the details of the voting process." Samir Chopra and Scott D. Dexter, *Decoding Liberation: The Promise of Free and Open Source Software* 169 (Routledge 2007).

[143] Cass R. Sunstein, *Free Markets and Social Justice* 322–326 (Oxford 1997). Nelson Rosenbaum explains that a major concern of the drafters of the Administrative Procedure Act of 1946 was the "perception that the interests of most citizens were being disregarded by a group of decision-making institutions that increasingly affected important aspects of their lives." Nelson M. Rosenbaum, *Citizen Participation and Democratic Theory*, in Stuart Langton, ed, *Citizen Participation in America: Essays on the State of the Art* 43, 45 (Lexington 1978). The statutory mandates authorizing citizen participation recognized the need to empower citizens to insure administrative fairness and accountability. Id.

[144] Sunstein, *Free Markets* at 322 (cited in note 143).

[145] Id. See also Rosenbaum, *Citizen Participation* at 48 (cited in note 143) ("Citizen participation can be extremely costly, unwieldy, and time-consuming.").

and security of critical automated systems, amplifying their officials' political accountability.

C. Political Accountability Facilitated

This proposal should also appeal to supporters of a strong executive model of administrative law. This model views presidential and gubernatorial influence over agency action as enhancing the administrative state's accountability by creating an "electoral link between the public and the bureaucracy."[146] Presidents and governors concern themselves with an agency's effectiveness because the public holds chief executive officers responsible for governmental performance.[147] Thus, executive officers and their senior staff work to ensure that agencies achieve their "objectives, without undue cost, in an expeditious and coherent manner" to ensure reelection.[148] The model contends that presidential administrations would be more likely to consider the preferences of the general public, rather than just parochial interests.[149]

This Article's proposal closes the information gap between a system's designers and the public, allowing the public to formulate more focused, informed complaints about a troubled system and to present those complaints to chief executive officers.[150] Senior executive staff could then respond to the public's specific concerns. The specificity of the public's complaints would make it harder for agencies to ignore them. At the same time, an open code approach would make it easier to hold an agency accountable for its response to such complaints.

---

[146] Sunstein, *Free Markets* at 322 (cited in note 143).

[147] See Elena Kagan, *Presidential Administration*, 114 Harv L Rev 2245, 2335 (2001); Cynthia R. Farina, *The "Chief Executive" and the Quiet Constitutional Revolution*, 49 Admin L Rev 179, 180-84 (1997) (addressing the impact of chief executives on "regulatory enterprise").

[148] Id. Advocates of this view argue it is equally applicable to executives whose desire for reelection is strong and to those who cannot serve again given their interest in their historical legacy. This view notes that the accountability point should not be overstated. The resolution of any particular regulatory issue plays a small role in the public's perception of presidential performance. See id.

[149] Sunstein, *Free Markets* at 325 (cited in note 143); D. Stephen Cupps, *Emerging Problems of Citizen Participation*, 37 Pub Admin Rev 478 (1977).

[150] This proposal would facilitate the transparency necessary for the operation of this model. Unlike software whose accuracy is unmistakably clear from its operation, such as life-critical systems like aircraft software, problems in closed code often remain hidden. In many instances, it may not be clear to the public that a problem even exists that needs correction.

Colorado's experience with CBMS demonstrates the point. In response to both a lawsuit filed by public interest groups about the failure of CBMS, and media coverage of the issue, Colorado's Governor created a new agency position charged with fixing CBMS.[151] Similarly, in 2007, California's Secretary of State launched an investigation of the state's e-voting systems after public interest groups expressed concerns about voter disenfranchisement.[152]

The next section explores how open code model would protect and amplify the expertise of agency decision-making.

D. Expertise Advanced

The technical community's input would advance the expertise model of administrative law, which emphasizes an agency's role in bringing specialized knowledge into the political domain.[153] An agency's expertise allows it to communicate with substantive experts, identify better experts, and assess which insights can be turned into workable administrative practices.[154] Agencies have the capacity to bring together specialized personnel and data, facilitating comprehensive analysis that generalist legislatures cannot match.[155] This model depends upon agencies having the necessary expertise and information available to it.[156]

The input of interested programmers could advance agency expertise in two critical ways. First, programmers could ensure that programming mistakes do not defeat an agency's own expertise. For instance, technicians working with public interest firms

---

[151] Bill Scanlon, *Benefits System Director Named*, Denver Rocky Mtn News 28A (May 28, 2005).

[152] See text accompanying notes 83–91.

[153] See Stephen G. Breyer, et al, *Administrative Law and Regulatory Policy: Problems, Text, and Cases* 182–85 (Aspen 6th ed 2006); Landis, *The Administrative Process* at 23–28 (cited in note 18) (explaining that expertise is a critical characteristic of agencies and the pressing need that engendered them).

[154] Stephen G. Breyer, *Breaking the Vicious Circle: Toward Effective Risk Regulation* 59–63 (Harvard 1993) (advocating a focus on expertise in administrative decisionmaking). Bruce Ackerman is another prominent advocate of focusing on expertise in administrative law. Bruce Ackerman, *The New Separation of Powers*, 113 Harv L Rev 633, 697–715 (2000).

[155] See Mashaw, *Due Process* at 19 (cited in note 2) (explaining that the creation of prominent administrative agencies emerged as a result of the need for more specialized expertise); Breyer, *Breaking the Vicious Circle* at 73–74 (cited in note 154).

[156] Mashaw, *Bureaucratic Justice* at 50 (cited in note 116) (explaining that the ideal of instrumental rationality in the context of particular administrative programs depends on a variety of conditions including whether administrators have all of the facts that are relevant to decisionmaking).

could catch programming errors that alter established policy in systems such as CBMS.[157] That feedback would allow an agency to insist that its vendor fix the code to reflect the agency's own policy choices.

Second, the technical community would provide agencies with crucial data to make optimal decisions. The expertise model extols agencies for their "capacity to bring together information on the beneficial and detrimental aspects of regulatory alternatives."[158] Closed systems prevent agencies from fulfilling that role. Open code would allow agencies to leverage the expertise of a broad technical community in making procurement decisions and in reviewing systems.[159] This proposal would provide an inexpensive means to enhance the expertise of agency decisionmaking.

Such expert input is particularly important for agencies that do not have access to such expertise either in-house or through outside advisors.[160] For instance, election officials currently lack sufficient information to conduct rigorous reviews of e-voting systems.[161] Election officials do not know enough about how the machines operate to assess them.[162] As the elections supervisor of Florida's Leon County explained: vendors control all of the information about their e-voting machines and will not "tell me that [ ] buggy software is why I can't get the right time on [the machines'] audit logs."[163] If the systems' vendors made the source codes public, computer scientists and academics could help local and state election officials in checking these systems.[164] In other cases, the technical community could assess data storage sys-

[157] See Citron, 85 Wash U L Rev (cited in note 8).

[158] McGarity, *Reinventing Rationality* at 114 (cited in note 4).

[159] See, for example, Joana Matos Penha-Lopes, *Why Use an Open Source E-Voting System?*, 37 Assoc for Computing Machinery Special Interest Group on Computer Sci Ed Bulletin 412 (Sept 2005); Bruce Schneier, *What's Wrong with Electronic Voting Machines?*, openDemocracy (Nov 9, 2004), available at <http://www.opendemocracy.net/media-voting/article_2213.jsp> (last visited Feb 24, 2008); Raba Technologies, *Trusted Agent Report: Diebold AccuVote-TS Voting System* (2004), available at <http://www.raba.com/press/TA_Report_AccuVote.pdf> (last visited Feb 24, 2008).

[160] But See Bamberger and Mulligan, 75 U Chi L Rev at 100 (cited in note 100) (attributing success of Chief Privacy Officer of Department of Homeland Security Nuala O'Connor Kelly to, in part, her ability to build a staff with varied privacy training and expertise who actively participated in privacy associations and conferences).

[161] Rubin, *Brave New Ballot* at 24 (cited in note 10).

[162] Thompson, *Voting Machines*, NY Times Magazine (cited in note 45).

[163] Id.

[164] Wagner Testimony at 4 (cited in note 28).

tems for security vulnerabilities.[165] Programmers could inspect systems to ensure that they comply with privacy laws.[166] In short, the technical community's feedback would promote an agency's expertness.[167]

III. OBJECTIONS TO AN OPEN CODE MODEL

This proposal, of course, is not free from serious objections. This Part evaluates three central concerns about an open code model and concludes that this proposal deserves adoption. First, this proposal may face implementation and cost constraints. Agencies may be unable to insist that their vendors reveal the source code under current contract terms. In that case, the cost of switching systems would be a serious concern. A new system may require investments in equipment and staff training.[168] For instance, the Census Bureau recently dedicated significant resources implementing CPS that it would not want to repeat.[169] Vendors also may raise their systems' cost if forced to reveal their source codes.

A switch, however, has the potential to reduce long-term costs, especially for troubled systems, such as e-voting machines and automated public benefits systems, which require substantial resources to fix. Over the past three years, Colorado has spent millions of dollars working on CBMS, which continues to be plagued by problems.[170] Texas's adoption of a flawed auto-

---

[165] Of course not all security leaks relate to a system's flaws. Some are attributed to human error like the Veterans Administration employee who took home a laptop containing millions of SSNs of veterans and the laptop was stolen. See David Stout, *Veterans Agency to Atone with Free Credit Monitoring*, NY Times A22 (June 22, 2006).

[166] Berry and Moss, 11 Info Polity at 30 (cited in note 104) (noting alternatives to available products that store user information in a more covert manner). See generally Solove, *The Digital Person* at 68–71 (cited in note 42).

[167] Christopher F. Edley, Jr., *Administrative Law: Rethinking Judicial Control of Bureaucracy* 22 (Yale 1990) (arguing that outside participation increases agency expertise by giving people affected by administrative rules the opportunity to be heard and by negating the tendency of agencies to exercise power in an arbitrary way).

[168] Lee, 9 Vand J Enter & Tech L at 73 (cited in note 112) (explaining that the costs of switching to a new system may be too high for governments to have an incentive to adopt an open code system).

[169] Horvath Email (cited in note 33) (explaining that "[h]aving just undergone the lengthy and difficult behind-the-scenes conversion to Blaise, we are unlikely to [move towards open source software and] repeat that process in the foreseeable future").

[170] Jerd Smith, *Audit: Costly Errors in Computer System for Benefits Had High Mistake Rate*, Denver Rocky Mtn News 4A (Apr 19, 2006) (explaining that errors in computing system may cost Colorado as much as $10 million); Bill Scanlon, *Millions Spent on Welfare Fix*, Denver Rocky Mtn News 6A (Sept 3, 2005) (explaining that CBMS is "clumsy to use, has great trouble generating reports, requires users to work around kinks and makes mistakes issuing benefits"); Scanlon, *Benefits System Director Named* at 28A (cited

mated public benefits system similarly wasted hundreds of millions of dollars, eventually requiring the state to replace its initial vendor with another firm.[171] Open code would allow agencies and their vendors to enjoy feedback about a system's accuracy and security from programmers whose services are virtually free.

Significantly, the benefits of a more transparent and legitimate system should not be undervalued. Open code would provide opportunities for public participation, political accountability, and expertise that are now absent. It might prevent the disenfranchisement of voters and ensure greater accuracy in decision-making systems. Agencies and legislatures should consider the short-term costs of a new system with the long-term savings of a more accurate, secure, and legitimate open system.

Critics may argue that vendors will refuse to build open systems that reveal their trade secrets. They may suggest that vendors will wait to see who moves first so they can free-ride on another's investments in research and development, resulting in stasis.[172] A first-mover problem, however, may be illusory for two reasons.

First, the high price tag of procurement contracts strongly suggests that vendors will design these systems. Because the government is the sole buyer in these markets, vendors will meet its conditions rather than dropping out of the market altogether. Indeed, in January 2008, Diebold spokesman Chris Riggall noted that "the company is considering making the software open source on its next generation of touch-screen machines" due to growing pressure from states.[173] As Riggall explains: "if the expectations of our customers change, we'll have to respond to that reality."[174]

Second, vendors already have embraced the open code model given its potential for lucrative contracts. For instance, Open Voting Solutions, an e-voting machine vendor whose source code would be publicly available, has submitted proposals to boards of elections in New York.[175]

---

in note 151) (noting decision to create a position to correct the problems with CBMS).

[171] Patrick Michels, *The Tale of TIERS: Lessons from the Epic Pursuit of the Perfect Records Management System* 29 Government Tech (eRepublic Sept 2007).

[172] Cindy Cohn of the Electronic Frontier Foundation raised this issue at the "Law in a Networked World" symposium.

[173] Thompson, *Voting Machines*, NY Times Magazine (cited in note 45).

[174] Id.

[175] See Open Voting Consortium Website Press Release, *Vendor Applies for Open Voting Consortium Certification* (Oct 15, 2006), available at <http://www.openvotingconsortium.org/node/82> (last visited Feb 24, 2008).

If a first-mover disadvantage does arise, then states could band together in a consortium to purchase systems, splitting the costs of research and development. A first-move disadvantage supports the OMB's involvement in this issue. The OMB could help coordinate purchasing or have federal agencies purchase en masse for all of the states that participate in programs that they run.[176] Between the software the OMB buys directly and that it funds, it dominates the market. Given the important public policy concerns at stake, the government has every right to use its market power to ensure that products meeting its specifications are available.

The second objection involves skepticism about whether this Article's proposal would generate the benefits that it promises. Some may question whether a broader technical audience would, in fact, review the source code of certain systems.[177] The typical open source project only has a small number of contributors.[178] That surely would not be true of high-profile systems, such as e-voting machines. As Professor Wagner has explained, and as past practice makes clear, open code e-voting systems would attract "the country's best independent technical experts to analyze the source code and publish their findings."[179] Such projects generate interest due to the reputational advantages of participating in such projects.[180]

Consider Australia's open code e-voting project. A private company designed Australia's e-voting system and posted all of the drafts of its source code online for review and criticism.[181] Interested programmers and independent auditors studied the source code and provided feedback.[182] An Australian National University professor caught the most serious problem.[183] The vendor, in turn, fixed the source code, shoring up the system's

---

[176] It is naturally true that states need a great deal of customization for systems depending upon how they administer a program and what policies they have selected for those programs.

[177] Jason Kitcat, *Source Availability and E-Voting: An Advocate Recants*, Commun of the Assoc for Computing Machinery 65, 66 (Oct 2004) (arguing that the more likely scenario is that the majority of open code would be ignored by the broader audience). Paul Ohm raised this concern at the "Law in a Networked World" symposium.

[178] Kitcat, *Source Availability* at 66 (cited in note 177).

[179] Wagner Testimony at 4 (cited in note 28).

[180] Sunstein, *Infotopia* at 148 (cited in note 116).

[181] Moynihan, 64 Pub Admin Rev at 524 (cited in note 45).

[182] Id.

[183] Id.

security.[184] Australia's e-voting system has received broad praise for its reliability and security.[185] Similarly, computer scientists working for the Open Voting Consortium have begun programming open source software for election systems in the United States.[186]

Systems affecting interest groups also would receive attention. One might imagine that public interest groups would direct significant energies to ensuring the accuracy of automated decision systems such as CBMS. Programmers might also review the source code for public benefits systems due to a sense that they are part of a meaningful social project.[187]

Although the chances of review are reduced for low-profile systems, the possibility is never completely absent or predictable. Indeed, computer security academics might ask students to assess such systems. Even if the source code of systems is not actually studied, important benefits remain. Those who believe that their work will be reviewed are more careful.[188] Due to the reputational costs of sloppy work, source code disclosure gives vendors a powerful incentive to ensure that their code is free of problems.[189] Thus, the open code model may inspire vendors to more thoroughly check the code's accuracy and security even for obscure programs.

The third objection concerns the security of open code systems. Software manufacturers argue that open code would enhance a system's vulnerability.[190] The computer security literature, however, rejects the notion that secrecy ensures a system's

---

[184] Id.

[185] Vaas, *U.S. E-voting Lags*, e-Week at 23 (cited in note 31); Kim Zetter, *Building a Better Voting Machine*, Wired (Oct 18, 2006), available at <http://www.wired.com/politics/security/news/2006/10/71957> (last visited Feb 24, 2008); Ananya Das, Yuan Niu, and Till Stegers, *Security Analysis of the eVACS Open Source Voting System* (2005), available at <http://wwwcsif.cs.ucdavis.edu/~stegers/eVACS-final-report.pdf> (last visited Feb 24, 2008).

[186] Open Voting Consortium, *The Solution: Open Voting*, available at <http://www.openvotingconsortium.org/> (last visited Feb 24, 2008).

[187] Sunstein, *Infotopia* at 160–62 (cited in note 116).

[188] As Jeremy Bentham initially observed, the fear of observation results in increased obedience and discipline. Solove, *The Digital Person* at 98 (cited in note 42); Michel Foucault, *Discipline and Punish: The Birth of the Prison* 200 (Pantheon 1977) (Alan Sheridan, trans). By contrast, vendors who keep their source code secret are more likely to be sloppy. Schneier, *Secrets and Lies* at 344 (cited in note 107).

[189] Wagner Testimony at 5 (cited in note 28).

[190] Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 Fordham L Rev 1711, 1794 (2005) (explaining the pros and cons of the "security through obscurity" approach taken by software users in restricting access to code).

safety.[191] This literature explains that security is not achieved by concealing security defects, but instead by allowing interested programmers to identify flaws that need to be fixed.[192] Open code enlarges the available pool of intelligence, enabling a community of testers to identify bugs and problems with the code.[193] Because it is more likely that flaws will be discovered if the source code is available for inspection, computer scientists advocate open e-voting systems.[194] The only security measures that must remain secret are a system's changeable secrets, such as its passwords and cryptographic keys.[195]

At the same time, revealing the source code incurs only a low-level of risk.[196] Unlike a warring nation that learns much from discovering an enemy's military plans, computer attackers learn little from the disclosure of a system's source code.[197] This is because computer security measures, such as firewalls, have a low level of uniqueness.[198] As a result, attackers can find a system's flaws without the source code.[199]

Studies demonstrate that open source software provides better security than proprietary software.[200] For this reason, agencies with salient security requirements, such as the Department

---

[191] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (Wiley 2d ed 1996); Schneier, *Secrets and Lies* at 344 (cited in note 107) (arguing that safety may not be ensured by a software's secrecy). Some computer scientists, however, suggest that whether a system is open or closed makes no difference as to security in the long run. See Hearing Before California Senate Elections Committee, *The Relative Merits of Openness in Voting Systems* (testimony of Peter G Neumann) (Feb 8, 2006), available at <http://www.csl.sri.com/users/neumann/calsen06.pdf> (last viewed Feb 24, 2008).

[192] Schneier, *Applied Cryptography* (cited in note 191).

[193] Eric S. Raymond, *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* 19 (O'Reilly rev ed 2001) ("Given enough eyeballs, all bugs are shallow."); Wagner Testimony at 4 (cited in note 28); Peter P. Swire, *A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?*, 3 J Telecommun & High Tech L 163, 169 (2005) (arguing that multiple users are more likely to identify and correct flaws in the code). A corollary point is that the soundness of a decision grows the more diverse the minds inspecting it. For a general discussion, see Sunstein, *Infotopia* (cited in note 116).

[194] Caltech/MIT Voting Technology Project, *Immediate Steps to Avoid Lost Votes in the 2004 Presidential Election: Recommendations for the Election Assistance Commission* (2004), available at <http://www.vote.caltech.edu/media/documents/EAC.pdf> (last visited Feb 24, 2008); Berry and Moss, 11 Info Polity at 26 (cited in note 104).

[195] Schneier, *Secrets and Lies* at 344 (cited in note 107).

[196] Swire, 3 J Telecommun & High Tech L at 168 (cited in note 193).

[197] Id at 168.

[198] Id.

[199] Id.

[200] Jaap-Henk Hoepman and Bart Jacobs, *Increased Security Through Open Source*, Commun of the Assoc for Computing Machinery 79, 81 (Jan 2007) ("We believe that open source software is a necessary requirement to build systems that are more secure.").

of Defense and the National Security Agency, have adopted Linux operating systems.[201] The Departments of Veterans Affairs, Defense, and Health and Human Services employ open source software to maintain patient health records.[202] California's Air Resource Board runs 65 percent of its databases on open source software for the security that it offers.[203]

This proposal, however, has its limits. It should not apply when the importance of secrecy outweighs the transparency, democratic legitimacy, and expertise open code brings. The exceptions to the Freedom of Information Act's ("FOIA") disclosure requirements provide insight into situations where public policy concerns might support a closed code regime.[204]

Consider these examples. FOIA excludes information compiled by law enforcement from public disclosure if producing such information would reveal "techniques and procedures for law enforcement investigations."[205] The IRS's auditing software might qualify as code that should remain closed in order to prevent individuals from gaming the system. The "No Fly" data matching program seemingly falls within FOIA's exemption from disclosure information that would "endanger the life or physical safety of any individual."[206] Its source code should not be opened on the grounds that terrorists could evade detection if they knew the system's logic.[207]

---

[201] Hal R. Varian and Carl Shapiro, *Linux Adoption in the Public Sector: An Economic Analysis* 10, (Dec 1, 2003), available at <http://www.sims.berkeley.edu/~hal/Papers/2004/linux-adoption-in-the-public-sector.pdf> (last visited Feb 24, 2008); John Rendleman, *Navy CIO OKs Open Source Systems*, Government Computer News (June 8, 2007), available at <http://www.gcn.com/online/vol1_no1/44441-1.html> (last visited Feb 24, 2008).

[202] The Veterans Administration received the Award for Innovation in American Government from the Ash Institute for Democratic Governance and Innovation at Harvard University's Kennedy School of Government for its health information system. U.S. Department of Veterans Affairs, *VistA Frequently Asked Questions* 1 (July 10, 2006), available at <http://www.innovations.va.gov/innovations/docs/InnovationsVistAFAQPublic.pdf> (last visited Feb 24, 2008). Patient health information is safeguarded with valid encryption system and secure access code. Id at 2.

[203] Ellen Perlman, *Open Sorcerer*, Governing (May 2006), available at <http://governing.com/articles/5open.htm> (last visited Feb 24, 2008) (explaining that open source code is less vulnerable to viruses than proprietary software). By contrast, a recent study of 227 information technology systems currently in use in the administrative state gave those systems failing marks for security. David A. Powner, US Government Accountability Office, Rep No GAO-07-1211T, *Information Technology: Further Improvements Needed to Identify and Oversee Poorly Planned and Performing Projects* 3 (2007) (explaining that nearly all of those systems employed closed, proprietary code).

[204] 5 USC § 552(b)(1)–(9) (2000 & Supp 2004). So too would exceptions to state open-record laws.

[205] 5 USC § 552(b)(7)(E).

[206] Id.

[207] See Citron, 85 Wash U L Rev at 1286 (cited in note 8) (arguing that algorithms of

To that end, this Article's proposal should provide a presumption of open code that could be rebutted by other important public policy concerns. Evidence of such public policy concerns, however, should be carefully reviewed. The administrative law values that an open code regime secures should not be forsaken without clear justification.

CONCLUSION

Critics of the administrative state are troubled by its opacity and lack of democratic pedigree. Agencies' closed information systems exacerbate these concerns. This Article argues that opening up the source code of these systems can combat these problems by illuminating agency decisions bound up in these systems. An open code model would secure the participation of a technical community that has previously played no role in the administrative state. And more importantly, this proposal would enhance the political accountability and expertise of agency decision-making.

"No Fly" program should be subjected to review of the Independent Advisory Board to ensure due process protections).