

2009

Individual Liberties and Intellectual Property Protection—Proprietary Software in Digital Electronic Voting Machines: The Clash Between a Private Right and a Public Good in an Oligopolistic Market.

Brenda Reddix-Small
Franklin Pierce Law School

Follow this and additional works at: <https://ir.lawnet.fordham.edu/iplj>



Part of the [Entertainment, Arts, and Sports Law Commons](#), and the [Intellectual Property Law Commons](#)

Recommended Citation

Brenda Reddix-Small, *Individual Liberties and Intellectual Property Protection—Proprietary Software in Digital Electronic Voting Machines: The Clash Between a Private Right and a Public Good in an Oligopolistic Market.*, 19 Fordham Intell. Prop. Media & Ent. L.J. 689 (2009).

Available at: <https://ir.lawnet.fordham.edu/iplj/vol19/iss3/2>

This Article is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Intellectual Property, Media and Entertainment Law Journal by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact tmelnick@law.fordham.edu.

Individual Liberties and Intellectual Property Protection—Proprietary Software in Digital Electronic Voting Machines: The Clash Between a Private Right and a Public Good in an Oligopolistic Market.

Cover Page Footnote

I would like to thank the faculty and staff of Franklin Pierce Law School for their invaluable support without which this publication would not have been possible. My sincerest thanks to my family, Milton, Khalfani, Emeka and Kay; and to my student researchers Linda Hyunh, T. Primianno, J. Damani, D. Silva and R. Woods.

Individual Liberties and Intellectual Property Protection – Proprietary Software in Digital Electronic Voting Machines: The Clash Between a Private Right and a Public Good in an Oligopolistic Market

Brenda Reddix-Small^{*}

ABSTRACT	690
INTRODUCTION	691
A. <i>The Oligopolistic Marketplace</i>	695
I. THE CONFLICT: BALANCING THE RIGHT TO VOTE VS. INTELLECTUAL PROPERTY RIGHTS	698
II. INDIVIDUAL LIBERTIES: CONSTITUTIONAL PROTECTION FOR THE RIGHT TO VOTE	707
III. HAVA AND THE PROVISION OF FUNDS	719
IV. INTELLECTUAL PROPERTY RIGHTS: COPYRIGHTS—FEDERAL PROTECTION FOR A PROPERTY INTEREST	723

A PDF version of this Article is available online at <http://law.fordham.edu/publications/article.ihtml?pubID=200&id=3022>. Visit <http://www.iplj.net> for access to the complete Journal archive.

* I would like to thank the faculty and staff of Franklin Pierce Law School for their invaluable support without which this publication would not have been possible. My sincerest thanks to my family, Milton, Khalfani, Emeka and Kay; and to my student researchers Linda Hyunh, T. Primianno, J. Damani, D. Silva and R. Woods.

690	<i>FORDHAM INTELL. PROP. MEDIA & ENT. L.J.</i>	[Vol. 19:689
	A. <i>Source Code and Object Code and Copyright Protection</i>	728
V.	TRADE SECRETS—STATE INTELLECTUAL PROPERTY PROTECTION	731
	A. <i>Oligopoly in the DRE Marketplace</i>	739
	1. The Prisoner’s Dilemma and Voting Rights	739
	CONCLUSION.....	764

ABSTRACT

The convergence of intellectual property protections afforded software, the fundamental liberty interests of voting rights of Americans and the conduct of voting machine vendors within an oligopolistic marketplace signals grave consequences for the public. In an election, Direct Recording Electronic voting machines (“DREs”) could be subject to malfunctions, inaccuracies and security problems. The DRE vendors have consistently failed to improve the voting machines or allow access for independent auditing and security testing. The vendors have operated collectively to maintain current inefficient output quality. Acting in concert to obtain higher pricing, the vendors operate against their individual self-interests, claiming proprietary protections. The result of this oligopoly is serious—the voting process, a public good, is diminished. Ultimately the federal judiciary and Congress will face the task of balancing these interests within the context of an oligopolistic marketplace. At risk is an American liberty.

INTRODUCTION

A small number of vendors¹ fueled by federal dollars² supply the majority of Direct Recording Electronic voting machines (or “DREs”)³ to states in federal elections.⁴ These few DRE vendors

¹ A handful of companies provide the majority of the voting machines to the states for federal elections including: Election Systems & Software (“ES&S”) (thirty-nine states), Premier (thirty-one states), Sequoia (eighteen states), Hart InterCivic (twelve states), MicroVote (three states), Advanced (two states). *See infra* Appendix I. Company names were provided in response to a Freedom of Information Request sent by the author to all fifty states, the responses of which are on file with the author.

² Help America Vote Act of 2002 (“HAVA”), Pub. L. No. 107-252, 116 Stat. 1666 (codified at 42 U.S.C. §§ 15301–545 (2006)). HAVA became public law on October 29, 2002. *Id.* Among other matters HAVA established a program to provide funds to states to replace punch card voting systems and provided minimum election administration standards for states and units of local government with the responsibility for the administration of federal election. *Id.* HAVA provided over three billion dollars to the states over four years to incentivize their transition to voting machine technology and to update election administration standards. See the U.S. Election Assistance Commission (“EAC”) for the list of vendors registering for certification under HAVA. 2006 U.S. EAC Ann. Rep. 22, available at http://www.eac.gov/about/report/docs/eac-20ar2006.pdf/attachment_download/file [hereinafter 2006 ANNUAL REPORT]; *see also* Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 *FORDHAM L. REV.* 1711, 1732 (2005) (“The legislation eventually enacted (HAVA) sets modest mandates for voting systems, while attempting to give the states incentives to upgrade to better technology. . . . Title I of HAVA authorizes \$650 million in payments to the states, half of which is for the replacement of punch-card ballots and lever voting machines. States that choose to receive payments under Title I are obligated to replace their punch card and lever voting equipment by November 2004 . . .”).

³ The terms ‘direct recording electronic’ voting machines and ‘digital recording electronic’ voting machines (“DREs”) are used interchangeably. *See* Michael A. Carrier, *Vote Counting, Technology and Unintended Consequences*, 79 *ST. JOHN’S L. REV.* 645, 646 (2005) (describing electronic voting machines by saying that “electronic voting machines [are] known as direct recording electronic devices (DREs)”; *see also* DIMITRIS A. GRITZALIS, *SECURE ELECTRONIC VOTING* 33 (2003) (“The fully computerized systems are of two formats—Direct Recording Electronic (DRE), where a voting kiosk (similar to an automatic bank teller machine) is provided at designated polling places, or networked systems that are used remotely, possibly via Internet/Web access.”); James Belmont Conn, *Race Against the Machine: An Argument for the Standardization of Voting Technology*, 12 *WASH. & LEE J. CIVIL RTS. & SOC. JUST.* 181, 231 (2006). Conn describes various voting technologies, such as Electronic Systems:

With electronic voting, voter choices directly enter electronic storage, using touch screens, push buttons or keyboards. Machines are typically programmed to prevent overvoting. The most common models are ‘full faced,’ showing all contests at once, like lever machines, and a flashing red light alerts voters to the contests in which they have not yet voted.

effectively operate as an oligopoly—controlling price and access.⁵ Simultaneously, within these DREs, the federally protected right to vote and the vendor's rights in intellectual property are clashing as competing interests.⁶

Scholars of divergent viewpoints have analyzed transparency, accuracy and software security issues attributable to electronic voting machines,⁷ including the lack of a paper ballot.⁸ Many

Id.

⁴ Using HAVA as a base, the fifty states were sent a Freedom of Information request, as this was the most straightforward method to track purchases made with federal funds since 2002, when the Act was passed. The fifty states purchased their direct electronic voting machine separately from the following most frequently named vendors: ES&S (thirty-nine states), the vendors which were formerly Diebold (thirty-one states), Sequoia (eighteen states), Hart InterCivic (twelve states). *See infra* Appendix I; BRENNAN CENTER TASK FORCE ON VOTING SYSTEM SECURITY, *THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD 2* (2006), available at http://brennan.3cdn.net/a56eba8edf74e9e12e_r2m6b86s2.pdf (providing a list of certified vendors).

⁵ *See infra* notes 18–26 and accompanying text.

⁶ *See infra* notes 28–37 and accompanying text.

⁷ Critics of electronic voting machines have identified the transparency, accuracy and integrity issues existing within direct electronic voting machines. *See* ERIC A. FISCHER, CONGRESSIONAL RESEARCH SERVICE, *ELECTION REFORM AND ELECTRONIC VOTING SYSTEMS (DRES): ANALYSIS OF SECURITY ISSUES* 26 n.101 (2003), <http://www.epic.org/privacy/voting/crsreport.pdf>, for a discussion of security issues inherent in the new electronic voting machines designed to facilitate increased voting with accuracy and transparency for the populace. *See, e.g.*, BEV HARRIS, *BLACK BOX VOTING: BALLOT TAMPERING IN THE 21ST CENTURY* (2004); AVIEL D. RUBIN, *BRAVE NEW BALLOT: THE BATTLE TO SAFEGUARD DEMOCRACY IN THE AGE OF ELECTRONIC VOTING* (2006); ROY G. SALTMAN, *THE HISTORY AND POLITICS OF VOTING TECHNOLOGY, IN QUEST OF INTEGRITY AND PUBLIC CONFIDENCE* (2006); Stephanie Philips, *The Risks of Computerized Election Fraud: When Will Congress Rectify a 38-Year-Old Problem?*, 57 ALA. L. REV. 1123 (2006); Tokaji, *supra* note 2; *see also* David Levine, *Secrecy and Unaccountability: Trade Secrets in our Public Infrastructure*, 59 FLA. L. REV. 135, 135 (2007).

⁸ Scholars claim that DREs with their inaccessible proprietary source code fail to provide the accuracy of reliable vote counting necessary for a transparent provision of a public good—voting. *See, e.g.*, Herbert E. Cihak, *The Help America Vote Act: Unmet Expectations?*, 29 U. ARK. LITTLE ROCK L. REV. 679, 684 (2007) (“It is not apparent that the EAC, or Congress for that matter, fully understood the nation-wide ramifications of replacing punch card voting machines, lever voting machines, and paper ballots with electronic touch screen voting equipment. As early as 1969, studies had surfaced which indicated that computerized voting presented a whole host of security issues. Coupled with electronic voting machine security is the issue of electronic machine malfunctions. A substantial number of voting machine failures were unveiled during the 2006 primary election season.”); Matthew Fisher, *Will Your Vote Count?: Can the Current Software Withstand and Guarantee the Constitutional Right to Vote?*, 8 J. HIGH TECH. L. 91, 105

comments have been written critiquing the lack of access to DRE proprietary software for independent testing and auditing purposes.⁹ However, the effect of the DRE vendor oligopoly on the price and access of DREs in the marketplace has not received comparable attention.

This Article contends that the lack of access to the proprietary software in the DREs is a function of market control exercised by the vendors.¹⁰ Furthermore, this Article argues that the DRE vendors are trapped in a Prisoner's Dilemma¹¹ concerning access to proprietary software as a function of the price of the voting

(2008) ("The fear of an outside attack on a DRE voting machine occupies much of the public alarm over the use of electronic voting. The possibilities for an attack on the software fit into three main categories, physical, code based, and result alteration."). *But see* Tokaji, *supra* note 2, at 1716 (opining that DREs are better solutions than the old paper-based systems).

⁹ See *supra* notes 6–8.

¹⁰ Joseph Kattan & William R Vigdor, *Game Theory and the Analysis of Collusion in Conspiracy and Merger Cases*, 5 GEO. MASON L. REV. 441, 443 n.6 (1997) ("By market conditions or market characteristics, we refer to all of the factors that bear upon the ability of firms to achieve, monitor competitors' adherence to, and punish deviations from an understanding. These include concentration, information availability and quality, firm differentiation, cost characteristics, product differentiation or homogeneity, technological stability, transaction characteristics, trade customs and usages, buyer characteristics, entry conditions, and the ability of fringe firms to expand, among others. The terms market conditions or market characteristics are used for convention and are not intended to suggest that one or more elements of market structure are determinative of market performance.").

¹¹ In the Prisoner's Dilemma,

two prisoners . . . are being interrogated separately, if each tries to blame the other, each is sentenced to eight years in prison; if both remain silent, each is sentenced to one year. If just one blames the other, he is released, but the silent prisoner is sentenced to ten years. The Prisoner's Dilemma is an example of a 2 by 2 game, because each of the two players . . . has two possible actions in his action set: Confess and Deny. Each player has a dominant strategy.

ERIC RASMUSEN, GAMES AND INFORMATION, AN INTRODUCTION TO GAME THEORY 21–20 (4th ed. 2006). This dominant strategy is one designed to maximize the individuals' outcome in this incarcerated situation. *Id.* "The Prisoner's Dilemma crops up in many different situations, including oligopoly pricing, auction bidding, salesman effort, political bargaining, and arms races. Whenever you observe individuals in a conflict that hurts them all, your first thought should be of the Prisoner's Dilemma." *Id.* at 21. However, if the two prisoners find a way to co-operate, then their outcome improves. *Id.* See *infra* notes 243–84 for a further explanation of the Prisoner's Dilemma.

machines. The dominant (best) strategy¹² for each individual DRE vendor normally would be to provide machines with software access at a price which maximizes profit. Based upon the demand by the states, this would be a rational decision on the part of the DRE vendors. The Nash equilibrium¹³ best position for each vendor ordinarily would be to deviate from any agreement among the vendors and provide access to the software to the voting public.¹⁴

However, as part of an oligopoly, (which acts like a monopoly) the dominant strategy for the DRE vendors collectively is to “cooperate” and withhold access to software and maintain market control over the purchase and sale of the electronic voting machines.¹⁵ Absent careful oversight, a few private interests, the vendor owners, who preclude access to independent software

¹² “A player’s dominant strategy is his strictly best response even to wildly irrational actions by the other players.” *Id.* at 20; *see also* MORTON D. DAVIS, *GAME THEORY, A NONTECHNICAL INTRODUCTION* 7 (1997) (“A strategy in game theory is a complete plan of action that describes what a player will do under all possible circumstances.”).

¹³ *See infra* note 266 for a discussion of the Nash equilibrium; *see also* Gregory J. Werden, *Economic Evidence on the Existence of Collusion: Reconciling Antitrust Law with Oligopoly Theory*, 71 *ANTITRUST L. J.* 719, 721 (2004) (“The key equilibrium concept in oligopoly theory is *Nash, non-cooperative equilibrium*, which in simple terms defines an equilibrium as a set of actions by players such that no player has an incentive to alter its action in light of the actions being taken by the other players. This concept was introduced by mathematician John F. Nash, Jr. in 1950, and it earned him a share of the 1994 Nobel Memorial Prize in Economics.”) (citing John Nash, *Non-Cooperative Games*, 54 *ANNALS OF MATHEMATICS* 286 (1951), *reprinted in* *COURNOT OLIGOPOLY* 82 (Andrew F. Daughety ed., 1988)).

¹⁴ Guy Sagi, *The Oligopolistic Pricing Problem: A Suggested Price Freeze Remedy*, *COLUM. BUS. L. REV.* 269, 277 (2008) (“The well known ‘prisoners’ dilemma game,’ represents the basic game theory payoff matrix. The famous paradox of this game is that both prisoners would have been better off, *ex ante*, if they could have reached a binding understanding to cooperate, but nevertheless the ‘Nash equilibrium’ of the game is to deviate. The classic prisoners’ dilemma game is a static, non-cooperative, one-shot-game. However, when the game repeats itself, the players can potentially establish a cooperative strategy that will benefit all. Cooperation comes about as a result of the players’ ability to retaliate in the following rounds if one player deviates from the mutually beneficial strategy to make a short-term profit. Consequently, deviating might become an unprofitable strategy.”).

¹⁵ *Id.* (“Oligopoly firms face a situation that resembles a contest or game. Each firm has to choose a strategy that will maximize its profits, taking into consideration its rivals’ strategies and reactions to the firm’s actions. Each firm’s profit depends upon its rivals’ strategies and therefore the logic guiding each firm’s decisions is within the domain of game theory.”).

testing could dictate the integrity and security of an American good: the public vote.¹⁶

To help understand and analyze the voting machine oligopoly, a quick examination of the marketplace looking at Game Theory¹⁷ and the conflict between voting rights and intellectual property (or “IP”) protection follows.

A. *The Oligopolistic Marketplace*

The term oligopoly is derived from the Greek words meaning a few sellers.¹⁸ Oligopolies are markets where only a few number of firms operate.¹⁹ These markets are not competitive, in that prices are higher than prices that would occur in competitive markets but lower than prices occurring in markets with a monopoly.²⁰

¹⁶ See *infra* notes 33–35.

¹⁷ DAVIS, *supra* note 12, at 3 (“The theory of games is a theory of decision making. It considers how one should make decisions and to a lesser extent, how one does make them.”); RASMUSEN, *supra* note 11, at 11 (“Game theory is concerned with the actions of decision makers who are conscious that their actions affect each other.”). Davis described the origin of game theory:

The foundations of game theory were laid by John von Neumann, who in 1928 proved the basic minimax theorem, and with the publication in 1944 of the *Theory of Games and Economic Behavior* the field was established. It was shown that social events can best be described by models taken from suitable games of strategy. These games in turn are amenable to thorough mathematical analysis.

DAVIS, *supra* note 12, at x.

¹⁸ MARIA MOSCHANDREAS, *BUSINESS ECONOMICS* 148 (2d ed. 1999). The few firms can either compete ruthlessly or collude and behave like a monopoly. If they collude, they form a cartel to reduce output and drive up profits the way a monopoly does. Howard A. Shelanski, *Adjusting Regulation to Competition: Toward a New Model for U.S. Telecommunications Policy*, 24 *YALE J. ON REG.* 55, 86 (2007).

¹⁹ Shelanski, *supra* note 18, at 86; see also Daniel R. Shulman, *Proof of Conspiracy in Antitrust Cases & the Oligopoly Problem*, 4 *SEDONA CONF. J.* 1, 14 (2003) (describing an oligopoly as “[s]ix or fewer sellers, or in some cases buyers, dominate, and merely through conscious parallelism are able to set prices without regard to costs or competitive forces” (citing *FTC v. Indiana Fed’n of Dentists*, 476 U.S. 447, 459 (1986) (decrying practices which impair “the ability of the market to advance social welfare by ensuring the provision of desired goods and services to consumers at a price approximating the marginal cost of providing them”))).

²⁰ *Id.* (“‘Oligopolies’ are markets that contain a small number of firms. Such concentrated markets are usually ‘imperfectly’ competitive: Oligopoly prices are generally higher than prices that result from perfect competition but lower than prices that result under monopoly.”).

Oligopolies are identified by behavior and resulting outcomes. In an oligopolistic market, the firms are few such that each firm makes its price and output decisions knowing its individual decisions will affect the market and cause reactions by other firms.²¹ Firms in oligopolies often earn profits higher than necessary to keep competitive firms in the industry, and they are not constrained by competition.²² In short, firms in an oligopoly do not have to accept the prices dictated by the marketplace.²³

This Article suggests that not only do the DRE vendors control the price, but they also prevent the independent review and testing of their product (voting machines) by precluding software access. This Article argues that this could only occur through cooperation and collective action by the vendors. This occurs even though DRE vendors provide a product traditionally created to be used as part of a public good (the voting process). As a result the opportunity for corruption of this public good remains in the hands of private concerns—an oligopoly fueled by a one-time federal infusion of capital.

The dictum in a Supreme Court case best summarizes a non-illegal definition of oligopolistic behavior as tacit collusion between firms:

²¹ Shelanski, *supra* note 18, at 86; RESEARCH AND EDUC. ASS'N, ECONOMICS: A COMPLETE SOLUTION GUIDE TO ANY TEXTBOOK 754 (1980) (“A market has an oligopolistic structure if actions by one firm have such important effects upon rivals that these rivals will contemplate appropriate reactions, which may affect the original firm. In other words, an oligopoly exists when each firm in an industry must contemplate the possible reactions of its rivals in deciding its own behavior.”).

²² Shelanski, *supra* note 18, at 86.

²³ *Id.* (“Firms in oligopolies thus often earn profits higher than necessary to keep competitive firms in the industry and are not constrained, as firms facing perfect competition are, to accept passively the prices dictated to them by the marketplace. The key feature of oligopolies, and the one that generates higher profits, is that there are few enough firms that each firm makes price and output decisions knowing its individual decisions will affect the market and cause responses by other firms. Anticipation of those competitive responses may cause a firm to rethink what at first looks like a profit-enhancing move.”). “Demand is defined as a schedule which shows the various amounts of a product which consumers are willing and able to purchase at each specific price in a set of possible prices during some specified period of time.” RESEARCH AND EDUC. ASS'N, *supra* note 21, at 480. Price then is the inverse function of said demand curve or schedule and represents the “monetary” amount that consumers are willing to pay for a specific amount of a product during some specified period of time. *Id.*

Tacit collusion, sometimes called oligopolistic price coordination or conscious parallelism, describes the process, not in itself unlawful, by which firms in a concentrated market might in effect share monopoly power, setting their prices at a profit-maximizing, supra-competitive level by recognizing their shared economic interests and their interdependence with respect to price and output decisions.²⁴

DRE vendors, by operating in a concentrated market and sharing monopoly power, set prices and control output decisions. Those decisions include preventing access, and possibly eliminating accuracy in the voting process in order to maximize supra-competitive profits.²⁵ This Article proposes to show that the balance of the competing interests of voting liberties and intellectual property rights is negatively impacted by this oligopolistic marketplace.

Game theory is a way of organizing a logical method of analyzing how two actors reach maximization of their profits, while considering the other firm's possible reactions and strategies²⁶ and can be useful in assessing the DRE marketplace. An analysis of various game theory applications shows that the dominant strategies for individual electronic voting machine owners would be to provide access for testing and independent auditing.²⁷

²⁴ Brooke Group Ltd. v. Brown & Williamson Tobacco Corp., 509 U.S. 209, 227 (1993).

²⁵ Thomas A. Piraino, Jr., *Regulating Oligopoly Conduct Under the Antitrust Laws*, 89 MINN. L. REV. 9, 54. Piraino opines that the structure of oligopoly markets encourages anti-competitive conduct by allowing the oligopolists to coordinate their behavior to maintain prices above the normal competitive level.

The weight of economic theory, however, now supports the conclusion that oligopolies do facilitate supracompetitive pricing. In 1838 Augustin Cournot published one of the first theses on oligopolistic behavior. In his model, two theoretical oligopolists calculate their output so that, together, they will be able to achieve a profit-maximizing price approaching the monopoly level.

Id. at 17.

²⁶ See generally Sagi, *supra* note 14, at 277.

²⁷ See *infra* text accompanying note 320.

In reality the DRE vendors are claiming copyright and trade secret protection and refusing to provide access or to alter the machines. Using game theory analysis, this conduct on the part of the DRE vendors leads to the inevitable conclusion that the vendors operating in this oligopoly are acting cooperatively and controlling market access. This constraint against auditing access occurs against a backdrop of the citizens' constitutional right to suffrage versus the intellectual property rights of the authors of the machines' source coding.

I. THE CONFLICT: BALANCING THE RIGHT TO VOTE VS. INTELLECTUAL PROPERTY RIGHTS

Two federally protected rights, subsisting within DREs, are currently in conflict as competing interests.²⁸ The right to vote in fairly conducted elections and the right to proprietary protection for IP are headed for a constitutional collision in elections using DREs.²⁹ As one scholar opines:

DRE voting machine manufacturers utilize proprietary code because this enables the manufacturers to take advantage of intellectual property protections, preventing substantive oversight. By gaining protection for the software,

²⁸ See Andrew Massey, "But We Have to Protect Our Source!": *How Electronic Voting Companies Proprietary Code Ruins Elections*, 27 HASTINGS COMM. & ENT. L.J. 233, 235 (2004) (identifying the conflict between the federal right to vote and the intellectual property protections granted to proprietary software in electronic voting machines).

²⁹ See Doris Estelle Long, *Electronic Voting Rights and the DMCA: Another Blast from the Digital Pirates or a Final Wake Up Call for Reform?*, 23 J. MARSHALL J. COMPUTER & INFO. L. 533, 548–89 (2005) ("Diebold's use of the DCMA [Digital Millennium Copyright Act] to prevent the publication of information regarding security concerns with its voting software puts the Copyright Act on a direct collision course with the First Amendment. . . . Nothing seems more 'political' than information about the reliability of voting machines, and, ultimately, the fairness of the election process."); Massey, *supra* note 28, at 234. Massey asserts that DREs pit the voting rights of the public against the proprietary rights of the software owners: "Unlike traditional paper-ballot systems . . . [DREs] record votes in secret, meaning that the voting public has no idea whether its vote counted, and if it did count, whether, it went to the person for whom the voters voted." *Id.*; see also Tokaji, *supra* note 2, at 1741–94 (providing a critique of clashing rights within electronic voting machines).

most likely through copyright the manufacturer of the DRE machine determines who can legally access and test the software. Permitting a private company to exercise complete control over voting software enables the same private actor to remove transparency from elections. The DMCA [Digital Millennium Copyright Act], enacted to update copyright laws for digital media, could potentially result in the copyright holder of voting software preventing any distribution of information about copyrighted material. The control granted by the DMCA also permits a software owner to limit security testing of the software to owners or operators, precluding the ability of outsiders, who may have more experience or time, from gauging the ability of voting software to protect the information generated during an election.³⁰

Both the right to vote and proprietary intellectual property rights are sufficiently important to our democracy as to have achieved federal protection, either in the Constitution or by congressional action.³¹ Yet the vendors of DREs and owners of

³⁰ Fisher, *supra* note 8, at 102; *see also* Long, *supra* note 29, at 540 (opining that proprietary source code with the help of the DMCA are in direct conflict with First Amendment rights and voting rights).

³¹ *See* Trevor Potter & Marianne Holt Viray, *Federal Election Authority: Jurisdiction and Mandates*, in *RETHINKING THE VOTE: THE POLITICS AND PROSPECTS OF AMERICAN ELECTION REFORM* 102, 103 (Ann N. Crigler, Marion R. Just & Edward J. McCaffery eds. 2004) (“The U.S. Congress has broad constitutional authority to regulate the times, places, and manner of federal elections As a result of this authority, as well as the authority to ensure equal protection of citizens’ voting rights in state and local elections, the federal government is already an active participant in establishing election rules on issues ranging from voter registration to enforcement of equal access to voting booths.”). *See also infra* notes 59–132 for a discussion of the right to vote under the Constitution. Intellectual property protection originates in the Constitution and state and federal legislation. *See, e.g.*, U.S. CONST. art. I, § 8, cl. 8 (the Patent and Copyright Clause); 17 U.S.C. § 4 (1909 Copyright Protection Act) (providing constitutional protection for patents and copyrights); Act of May 31, 1790, ch. 15, 1 Stat. 124; Act of March 3, 1891, ch. 565, 26 Stat. 1106 (extending copyright protection to foreign nationals and imposing copyright registration formalities); WENDY J. GORDON & RICHARD WATT, *INTRODUCTION TO THE ECONOMICS OF COPYRIGHT: DEVELOPMENTS IN RESEARCH AND ANALYSIS passim* (2003) (providing a discussion of the property rights theories supporting the use of intellectual property protections); *see also infra* notes 151–234.

proprietary software, receiving substantial public funds, have managed to protect intellectual property rights at the expense of voting rights.³²

The voting rights process in federal elections involves the provision of a public good,³³ which in turn implicates the core values of citizen participation: transparency and equality of access.³⁴ Admittedly, intellectual property rights benefiting voting machine vendor owners may promote innovation, profit

³² See generally Massey, *supra* note 28, at 235. See Levine, *supra* note 7, at 138 (“But in late 2005, potential vendor Diebold . . . focused instead on its commercial property rights. Rather than comply with the law, it brought a declaratory judgment action against the state, arguing that it could not supply the required information. Diebold explained that some of the inner workings of its voting machines were a third party’s intellectual property, likely trade secrets, to which it did not have access. Therefore, Diebold claimed the information could not be shared with the state or the public without violating intellectual property rights or intellectual property licensing agreements with third parties, even if it had access to this information.” (citations omitted)); see also Long, *supra* note 29, at 541 (suggesting that the copyright protections of the source code under the DCMA are in conflict with the constitutional values of political speech and the integrity of the voting process); Tokaji, *supra* note 2, at 1779–80 (expressing concerns about the lack of auditing transparency because of both security and accuracy concerns).

³³ See James Love & Tim Hubbard, *Paying For Public Goods*, in CODE: COLLABORATIVE OWNERSHIP AND THE DIGITAL ECONOMY 207 (Rishab Aiyer Ghosh ed. 2005) (“Among economists, a public good is one that, regardless of its cost to produce, is not rival in consumption. That is to say, the marginal cost of sharing the good is zero, and the use of the good by an additional person does not diminish the availability of the good to others. Another aspect of the economics definition concerns the ability to prevent others from benefiting from the good—sometimes referred to as non-exclusivity of consumption.”).

³⁴ Levine, *supra* note 7, at 136 (“Transparency and accountability, especially in the last several decades, are among the core values that drive the fundamental model of a publicly elected and properly operating democratic government.”); see also Massey, *supra* note 28, at 235 (“The proprietary nature of the code requires a closed state review process that has not eliminated serious errors and security flaws because it limits the number of people testing the software. That closed process also contradicts public policy and American tradition favoring openness through transparent and accountable government. As a result, the electorate is forced to rely upon arguably substandard machines to conduct one of the most important functions of our democratic system.”); Lilian Mitrou et al., *Electronic Voting: Constitutional and Legal Requirements*, in SECURE ELECTRONIC VOTING 54 (Dimitris A. Gritzalis ed. 2003) (“A key element of democratic, free and fair elections is the trust and legitimization that is gained having a transparent vote casting and counting procedure.”).

maximization and a dynamic marketplace by securing protection for software in direct recording voting machines.³⁵

However, intellectual property laws protect the owners of proprietary software in DREs,³⁶ without adequately safeguarding the voter's right to a secure, fair and fraud-free election.³⁷ Despite reports questioning the security and transparency of electronic

³⁵ See U.S. CONST. art. I, § 8, cl. 8 (the Patent and Copyright Clause). In *Mazer v. Stein*, 347 U.S. 201 (1954), the Supreme Court identified one of the principles upon which the Copyright Clause was based: economics. *Id.* at 219. The Court opined that the policy behind the Clause was to promote public welfare through private market incentives. *Id.* “The economic philosophy behind the clause empowering Congress to grant patents and copyrights is the conviction that encouragement of individual effort by personal gain is the best way to advance the public welfare through the talents of authors and inventors in ‘Science and the useful Arts.’” *Id.*; see also GORDON & WATT, *supra* note 31, at xvi (“In the absence of legal protection, a writer might be afraid of showing his manuscript to a publisher lest it be copied, without payment . . . without copyright the situation could resemble a prisoner’s dilemma So a lack of copyright might lead to lack of payment and incentives for authors, and thus underproduction.”). See generally William Landes & Richard Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325 *passim* (1989).

³⁶ See Fisher, *supra* note 8, at 102; Massey, *supra* note 28, at 234–35 (“The source of this problem is the proprietary source code that drives these paperless electronic voting machines. Unlike paper-based voting machines, DREs operate entirely by computer, meaning that at no stage of the election process can the public see the physical counting of the votes. Absent access to the source code that runs the DRE, the public has no way of knowing how—or if—the machine records and tabulates votes. As a result, a growing chorus of critics claim that without the ability to scrutinize the process, the public has no way to protect against malicious manufacturers, elections officials, or voters from ‘hacking’ the machines to ‘deliver’ votes to their chosen candidates.”).

³⁷ Numerous reports and articles have been written concerning security flaws in DREs. See, e.g., RUBIN, *supra* note 7; Carrier, *supra* note 3, at 660 (“Another type of data fraud targets the record of all cast votes. Anyone with access to this data could alter vote records and ‘generate or change as many votes as he or she pleased.’ Such votes ‘would be indistinguishable from the true votes cast on the terminal.’ But despite the critical importance of the vote records, one single DATA Encryption Standard (“DES”) key, f2654hD4, has encrypted all of Diebold’s vote records data since 1998.”); Massey, *supra* note 28, at 235 (“In practice, proprietary code-based DREs have proven to be error-ridden and prone to security weaknesses because the closed nature of the code has forced state agencies to protect manufacturers’ intellectual property at the expense of a reliable voting system.”); DAVID JEFFERSON ET AL., A SECURITY ANALYSIS OF THE SECURE ELECTRONIC REGISTRATION AND VOTING EXPERIMENT (“SERVE”) *passim* (2004), <http://www.servesecurityreport.org/paper.pdf>; MICHAEL A. WERTHEIMER, DIEBOLD ACCUVOTE-TS VOTING SYSTEM *passim* (2004), http://euro.ecom.cmu.edu/program/courses/tcr17-803/TA_Report_AccuVote.pdf; Massachusetts Institute of Technology News Office, Voting Technology Fact Sheet, July 16, 2001, <http://web.mit.edu/newsoffice/2001/voting2facts.html>.

voting machines, Congress has failed to enact measures to require that DREs used in federal elections possess minimum software security protections.³⁸

In 2002, Congress passed HAVA to encourage states to upgrade voting technology and to increase the use of electronic voting machines.³⁹ HAVA funneled over three billion dollars to states to assist in this technological transition.⁴⁰ This federal infusion of monies into the private marketplace created a monetary incentive for states to purchase new voting machine technology.⁴¹

In an effort to address the security issues with DREs, Congress proposed additional legislation mandating audits and banning the use of DREs not retrofitted with voter verified paper ballots in

³⁸ See Carrier, *supra* note 3, at 646–47. Carrier asserts that Congress passed “‘HAVA,’ which provided \$325 million to the states to replace their punch card voting systems,” but that the Act does not remedy major deficiencies in electronic voting such as reduced transparency, with the possibilities of hidden trap doors in software eliminating millions of votes; increased magnitudes of error and fraud; and the lack of security controls, which “makes it astonishingly easy to change vote totals, register votes for unintended candidates, prematurely terminate elections, and erase the ‘audit log’ that is designed to trace such activity.” *Id.* at 646–47.

³⁹ HAVA, Pub. L. No. 107-252, 116 Stat. 1666 (codified at 42 U.S.C. §§ 15301–545 (2006)). The bill passed Congress in 2002 in the wake of the presidential election of 2000 where antiquated election administration and technology led to a national crisis during the election. See Daniel Palazzolo, Vincent G. Moscardelli, Meredith Patrick & Doug Rubin, *Election Reform after HAVA: Voter Verification in Congress and the States*, 38 PUBLIUS: THE JOURNAL OF FEDERALISM 515, 515 (2008), available at <http://publius.oxfordjournals.org/cgi/reprint/38/3/515.pdf>. HAVA was designed to encourage the states to adopt and upgrade their election technology. See *supra* text accompanying note 39.

⁴⁰ See Brian Kim, *Help America Vote Act*, 40 HARV. J. ON LEGIS. 579, 589 (2003) (“Title I of the Act contains provisions for replacing punch card machines and improving election administration. The Act allocates \$3.86 billion to states and localities to, among other things, improve the administration of federal elections, educate citizens about voting rights and procedures, train election officials and poll workers, improve or replace voting technology, and increase the availability of absentee ballots to overseas military voters. For the first time, substantial amounts of federal funds will be used to help finance federal elections.”); 2006 ANNUAL REPORT, *supra* note 2, at 22; Tokaji, *supra* note 2, at 1733.

⁴¹ See Carrier, *supra* note 3, at 646 (explaining that “[m]any states have enthusiastically embraced” Congress’s invitation in HAVA by replacing punch cards with DREs).

federal elections.⁴² However, this proposed amendment to HAVA never passed.

HAVA currently provides only limited safeguards for voter security. Through copyright⁴³ and trade secret⁴⁴ protection, DRE manufacturers protect their software from competition and outside scrutiny.⁴⁵ Without access to source code disclosure,⁴⁶ encryption⁴⁷ standards and mandated independent random audits,⁴⁸

⁴² See S. 1487, 110th Cong. (2007) (Senate bill “[t]o amend the Help America Vote Act of 2002 to require an individual, durable, voter-verified paper record under title III of such Act”); H.R. REP. NO. 110-154, at 2 (2007) (House Report accompanying “[a] bill to amend the Help America Vote Act of 2002 to require a voter-verified permanent paper ballot under title III of such Act, and for other purposes”). These bills never passed Congress.

⁴³ See Fisher, *supra* note 8, at 102 (“By gaining protection for the software, most likely through copyright, the manufacturer of the DRE machine determines who can legally access and test the software.”); Long, *supra* note 29, at 548–49; see also Kevin C. Earle, *No-Copy Technology and the Copyright Act: Has the Music Industry Been Allowed To Go Too Far In Diminishing The Consumers' Personal Use Rights In The Digital World?*, 2 J. MARSHALL REV. INTEL. PROP. L. 337, 341–42 (2003) (“Not only does the Federally codified Copyright Act encourage creation and dissemination of intellectual works for the public welfare, but it also provides exclusive rights and rewards to the copyright owners. Thus, the Copyright Act was drafted to balance certain public interests by granting access to protected copyright materials while simultaneously reserving certain proprietary rights to authors of original works.”).

⁴⁴ See J. THOMAS MCCARTHY ET AL., MCCARTHY’S DESK ENCYCLOPEDIA OF INTELLECTUAL PROPERTY 617–18 (3d ed. 2004) (defining a trade secret as “[b]usiness information that is the subject of reasonable efforts to preserve confidentiality and has value because it is not generally known in the trade” and noting that “[s]uch confidential information will be protected against those who obtain access through improper methods or by a breach of confidence”); see also MARK A. LEMLEY ET AL., SOFTWARE AND INTERNET LAW 4 (3d ed. 2006) (“One way for vendors to prevent users from freely copying their computer programs was to claim a program as a trade secret.”); *infra* notes 203–30.

⁴⁵ See Massey, *supra* note 28, at 241–44.

⁴⁶ See MICHAEL D. SCOTT, LICENSING AND INTELLECTUAL PROPERTY DESK REFERENCE 746–47 (2004) (“‘Although ‘source code’ has been defined far more broadly in some of the literature in the field, and in some of the expert testimony in this case, more commonly the term ‘source code’ refers to a computer program written in some programming language . . . that uses complex symbolic names, along with complex rules of syntax.’” (quoting *Lotus Dev. Corp. v. Paperback Software Int’l*, 740 F. Supp. 37, 44 (D. Mass. 1990))).

⁴⁷ See EPIC CRYPTOGRAPHY & LIBERTY SOURCEBOOK 1997 E-30 (David Banisar ed., 7th ed. 1997) (“Through the use of cryptography, communication and information stored and transmitted by computers can be protected against interception Modern encryption technology—a mathematical process involving the use of formulas or algorithms—was traditionally deployed most widely to protect the confidentiality of

proposed DRE legislation fails to provide for a fair, accurate and reliable voting system.⁴⁹

Scholars have argued for the use of voter verified paper trails (or “VVPTs”) in the voting process.⁵⁰ VVPTs require that the voting machine issue a paper receipt indicating how a voter cast her ballot. In the absence of public bid procedures for open source software⁵¹ in DREs, VVPTs simply do not offer a solution to the

military and diplomatic communications. With the advent of the computer revolution and recent innovations in the science of encryption, a new market for cryptographic products has developed.”); *see also* 47 U.S.C. § 605(d)(3) (2006) (defining “encryption” as “to transmit such programming in a form whereby the aural and visual characteristics (or both) are modified or altered for the purpose of preventing the unauthorized receipt of such programming by persons without authorized equipment which is designed to eliminate the effects of such modification or alteration”).

⁴⁸ *See Carrier, supra* note 3, at 654–56 (“The completely paperless nature of DREs, along with the role of computers in each stage of the vote counting process, ensures that, of the five types of voting technologies, DRE fraud is least likely to be detected and most likely to have vast effects. In addition, DRE fraud is possible at each stage of the voting process: before the election (through physically unsecured machines), during voting (through smartcards that allow voters to gain unauthorized access), and after votes have been cast (through votes that are misrecorded when registered or tabulated). . . . For all of these reasons, the testing and certification process is critical. Nonetheless, this process is flawed. For starters, there is a ‘stunning lack of transparency’ surrounding testing and certification, which the companies complete in secret and refuse even to discuss.”).

⁴⁹ *See Massey, supra* note 28, at 235 (“In practice, proprietary code-based DREs have proven to be error-ridden and prone to security weaknesses because the closed nature of the code has forced state agencies to protect manufacturers’ intellectual property at the expense of a reliable voting system.”). Massey argues for the mandated “use of open source code to ensure transparency and accountability mandated by law. In addition, states must eliminate escrow requirements to allow for public testing of the source code.” *Id.* at 236.

⁵⁰ *See Carrier, supra* note 3, at 647 (proposing “electronic voting machines[,] a voter-verified paper trail, random audits, open source software, [and] more robust certification” for the DREs).

⁵¹ STEPHEN J. DAVIDSON, STUART D. LEVI & LAWRENCE ROSEN, OPEN SOURCE SOFTWARE 2007: RISKS, REWARDS AND PRACTICAL REALITIES IN THE CORPORATE ENVIRONMENT 128 (2004) (“Open Source Software is software for which the underlying programming code is available to the users so that they may read it, make changes to it, and build new versions of the software incorporating their changes. There are many types of Open Source Software, mainly differing in the licensing term under which (altered) copies of the source code may (or must) be redistributed.” (citation omitted)).

Open source software is typically distributed under two kinds of licenses: BSD or GPL. Under the BSD license, a user may modify, recompile, and distribute the source code, so long as the original copyright is acknowledged. By contrast, under the GPL license, a user may likewise modify, recompile and distribute the source code,

problem of privately held software lacking independent access for review.⁵²

As the authors of the Brennan Center for Justice, Election Results noted:

The widespread adoption of voter-verifiable paper records does not, however, resolve the security, reliability, and verifiability issues with electronic voting that many groups, including the Brennan Center, have identified. To the contrary, as the Brennan Center noted in its June 2006 comprehensive study of electronic voting system security *The Machinery of Democracy: Protecting Elections in an Electronic World*, voter-verifiable paper records by themselves are “of questionable security value.” Paper records will not prevent programming errors, software bugs or the introduction of malicious software into voting systems. If paper is to have any real security value, it must be used to check, or “audit,” the voting system’s electronic records.⁵³

DREs store votes electronically, with the votes being submitted periodically throughout the election or collected on data storage cards.⁵⁴ This information is transmitted over a network connection or via Internet to a central location for tallying.⁵⁵ A software malfunction could trigger a number of problems including shutting

but does not have to acknowledge a copyright, and more importantly, cannot claim any copyright for the altered source code. The GPL license is the more prevalent of the two schemes, and is used in the popular Linux operating system to facilitate input from programmers interested in improving the system.

Massey, *supra* note 28, at 240 n.39.

⁵² See Massey, *supra* note 28, at 236 (arguing that the VVPT is subject to the same risks as existing paper based voting systems and “does nothing to further the general goal of restoring legitimacy to voting”).

⁵³ LAWRENCE NORDEN, AARON BURSTEIN, JOSEPH LORENZO HALL & MARGARET CHEN, BRENNAN CENTER FOR JUSTICE, POST-ELECTION AUDITS: RESTORING TRUST IN ELECTIONS 2 (2007), <http://electionaudits.org/files/Brennan%20Center%20Report%20on%20Post-Election%20Audits.pdf>.

⁵⁴ See Fisher, *supra* note 8, at 96.

⁵⁵ See Tokaji, *supra* note 2, at 1777.

down, counting two votes for every one vote and erasing entire numbers of votes from designated precincts. A VVPT could not assure that the all votes are counted or even counted accurately.⁵⁶

As a result of the current proprietary protection for electronic voting machine software, a few private interests⁵⁷ could dictate the security and integrity of American federal elections. The result: an oligopolistic control of a public good—the democratic election process.⁵⁸

This Article will examine the interplay between the oligopoly held by DRE vendors, the intellectual property rights subsisting within the electronic voting machines, and the conflict between fundamental voting rights. This Article proposes to do so by: (1) reviewing the right to vote and its place as a fundamental liberty; (2) examining the IP rights within DREs (copyrights and trade secrets); and (3) analyzing the marketplace for the oligopolistic effects of the DRE vendors.

Ultimately this Article argues that intellectual property (copyright and trade secret) protections for voting machine software undermine the gains made by voting rights advocates during the past forty years. More specifically, this Article contends that the creation of this oligopoly produces a market inefficiency (eliminating transparency, accuracy and voter participation) which prevents the public from controlling a public good and reaching a satisfactory balance between the two important interests.⁵⁹

⁵⁶ See NORDEN ET AL., *supra* note 53, at 46–59.

⁵⁷ The major vendors of digital recording voting machines include the following firms: ES&S, Premier, Sequoia, Hart InterCivic, MicroVote, Advanced. See *supra* note 1 and accompanying text.

⁵⁸ See Massey, *supra* note 28, at 235.

⁵⁹ See Daniel R. Ortiz, *The Paradox of Mass Democracy*, in RETHINKING THE VOTE: THE POLITICS AND PROSPECTS OF AMERICAN ELECTION REFORM 210, 210 (Ann N. Crigler, Marion R. Just & Edward J. McCaffery eds. 2004) (“Most of us agree, however, that any truly democratic system must at a minimum meet three necessary conditions: (1) relatively wide, if not universal, suffrage; (2) a great degree of equality among those allowed to vote; and, perhaps most controversially; (3) some degree of thoughtfulness among voters.”).

II. INDIVIDUAL LIBERTIES: CONSTITUTIONAL PROTECTION FOR THE RIGHT TO VOTE

The right to vote in a fairly conducted election is a constitutionally protected feature of United States citizenship.⁶⁰ Congress has the power to regulate federal elections pursuant to Article I, Section 4 of the U.S. Constitution (the Elections Clause)⁶¹ and Article I, Section 8, Clause 18 (the Necessary and Proper Clause).⁶² Based upon the utilization of voters' registration requirements for federal elections, which are co-extensive with state election registration requirements and election processes, the federal guarantees for a fairly conducted election have been broadened to include state and local election processes.⁶³

A number of constitutional amendments and attendant statutes create and protect the right to vote.⁶⁴ Carved out of historical

⁶⁰ See generally *Reynolds v. Sims*, 377 U.S. 533 (1964). The Supreme Court in *Reynolds* invalidated an apportionment scheme in the state of Alabama. *Id.* at 568. The Court held that the right to vote was a fundamental interest based upon the fact that the right to vote preserves all other rights. *Id.* at 560. The Court held that the apportionment scheme, which relied on a sixty year old census, diluted a citizen's right to vote based strictly on residency. *Id.* at 562. This dilution was deemed to be a violation of the Equal Protection Clause of the Fourteenth Amendment. *Id.* at 568. The Court struck down the apportionment scheme and required that a bicameral system for apportionment be instituted such that representation be based on "one person, one vote." *Id.* at 587. *Reynolds* was historic for its use of federalism to enforce a right to vote within a state election system. See *id.* at 574.

⁶¹ See U.S. CONST. art. I, § 4 ("The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Place of Chusing Senators."); see also *id.* art. II, § 1 (providing for states to choose electors for President and Vice-President).

⁶² *Id.* art. I, § 8, cl. 18.

⁶³ See CRAIG C. DONSANTO, IFES POLITICAL SCIENCE WHITE PAPER SERIES, PROSECUTION OF ELECTORAL FRAUD UNDER UNITED STATES FEDERAL LAW 3, http://www.moneyandpolitics.net/researchpubs/pdf/IFES_Nigeria_fraud_paper.pdf (explaining that the federal jurisdictional prerequisite is satisfied when a federal candidate is on the ballot or conduct occurs which impacts the voter registration process for a federal election or in a state where a person registers to vote simultaneously for federal as well as state and local offices).

⁶⁴ See, e.g., U.S. CONST. amend. XV; *id.* amend. XIV; 42 U.S.C. § 1973(a), (b) (2006) ("Denial or Abridgement of Right to Vote on Account of Race or Color Through Voting Qualifications or Prerequisites; Establishment of Violation"); *id.* § 1973gg-9 ("Civil Enforcement and Private Right of Action"). The 1965 Voting Rights Act (or "VRA") was hotly contested and fiercely litigated. See generally *American Civil Liberties Union*,

movements for suffrage, protections for the right to vote have been addressed extensively by the Supreme Court.⁶⁵

ACLU Voting Rights Project Litigation, <http://www.aclu.org/votingrights/gen/36949res20080929.html> (last visited Jan. 30, 2009). The VRA contains what is known as a preclearance requirement. The preclearance provisions (commonly known as “section 5 Preclearance”) require certain jurisdictions that used a discriminatory test or device for voting and in which voter registration or voting was depressed to preclear all their proposed changes in voting laws or practices. See Laughlin McDonald, *Racial Fairness—Why Shouldn’t It Apply to Section 5 of the Voting Rights Act?*, 21 STETSON L. REV. 847, 848 (1992) (“Preclearance requires these jurisdictions to prove to federal officials that the changes do not have the purpose and will not have the effect of discriminating on account of race or color or membership in a language minority. Voting changes that are denied preclearance are ineffective as law and are unenforceable.”).

Other provisions of the Act include: 42 U.S.C. § 1973, prohibiting voting practices that ‘result’ in discrimination; 42 U.S.C. § 1973b, abolishing ‘tests or devices’ for voting; 42 U.S.C. § 1973j, establishing criminal penalties for violations of the Act; 42 U.S.C. § 1973aa-6, establishing the right of disabled or illiterate persons to receive assistance in voting; 42 U.S.C. § 1973aa-1, abolishing durational residency requirements and establishing uniform standards for absentee voting in presidential elections; 42 U.S.C. § 1973d, f, providing for the appointment of federal examiners and observers; and, 42 U.S.C. § 1973b, 1973aa-1a, providing for special assistance to language minorities.

Id. at 852 n.35; see also U.S. CONST. amend. XIX (prohibits denial based on sex); *id.* amend. XXIV (eliminates poll tax); *id.* amend. XXVI (provides suffrage to persons eighteen years or older).

⁶⁵ See, e.g., *City of Rome v. United States*, 446 U.S. 156, 187 (1980) (upholding the constitutionality of the 1965 Voting Rights Act and banning electoral changes which have both the intent and effect of discriminating against African Americans); *Kramer v. Union Free Sch. Dist.*, 395 U.S. 621, 630, 633 (1969) (eliminating property requirements for eligibility to vote in a school district); *Katzenbach v. Morgan*, 384 U.S. 641, 646–47 (1966) (upholding the validity of 4(e) of the 1965 Voting Rights Act banning discrimination in voting); *Harper v. Va. Bd. of Elections*, 383 U.S. 663, 665, 667 (1966) (holding states have the authority to establish the basic terms of voting conditions, but conditions that burden the franchise of voting will be “carefully and meticulously scrutinized” and that wealth is not a qualification for voting); *Baker v. Carr*, 369 U.S. 186, 197–98 (1962) (subjecting district gerrymandering to federal court scrutiny and holding that it presented a justiciable question where voting issues are impacted); *United States v. Classic*, 313 U.S. 299, 322, 325 (1944) (finding that a vote is entitled to constitutional protection and a person cannot be denied that right to vote in a primary election and then have his vote count in a federal election); *Yick Wo v. Hopkins*, 118 U.S. 356, 370 (1886) (holding that the right to vote although not mentioned in the Constitution is a right which preserves all other rights); see also RUSSELL L. WEAVER, STEVEN I. FRIEDLAND, CATHERINE HANCOCK, DONALD E. LIVELY & WENDY B. SCOTT, *CONSTITUTIONAL LAW: CASES, MATERIALS & PROBLEMS* 561 (2006) (“Notably missing from the Fourteenth Amendment’s ambit of concern, as initially framed, was the right to

The phrase “right to vote” is not found in the United States Constitution.⁶⁶ Yet the right to vote is a fundamental liberty under which all other rights are exercised as articulated by the Supreme Court in *Reynolds v. Sims*⁶⁷ and *Harper v. Virginia State Board of Elections*.⁶⁸ Under the Fourteenth Amendment’s Equal Protection Clause, the *Harper* Court held that the right to vote is fundamental and entitled to a strict scrutiny review because it protects all other rights.⁶⁹ The *Reynolds* Court held that the right to vote freely for the candidate of one’s choice is the essence of a democratic society, and any restrictions on that right strike at the heart of a representative government.⁷⁰ At issue in *Reynolds v. Sims* was the state of Alabama’s apportionment scheme and whether it constituted discrimination under the Equal Protection clause.⁷¹ The Court scrutinized restrictions on the right to vote and articulated that

the right of suffrage is a fundamental matter in a free and democratic society. Especially since the right to exercise the franchise in a free and unimpaired manner is preservative of other basic civil and political rights, any alleged infringement of the right of citizens to vote must be carefully and meticulously scrutinized.⁷²

Congress also has the power to provide states with federal funds to implement federal acts, such as those protecting the right to vote, through Article 1, Section 8, Clause 1 (the General

vote. Its omission reflected the reality that the constitutional impact would touch not only the South but the North.”). See generally J. MORGAN KOUSSER, *COLORBLIND INJUSTICE: MINORITY VOTING RIGHTS AND THE UNDOING OF THE SECOND RECONSTRUCTION* (1999) (discussing voting rights, historical challenges and racially institutionalized discrimination practices affecting minorities in America).

⁶⁶ See *Yick Wo*, 118 U.S. at 370.

⁶⁷ *Reynolds v. Sims*, 377 U.S. 533, 561–62 (1964).

⁶⁸ *Harper*, 383 U.S. at 665–66.

⁶⁹ See *id.* at 667; Karyn L. Bass, Notes and Comments, *Are We Really Over the Hill Yet? The Voting Rights Act at Forty Years: Actual and Constructive Disenfranchisement in the Wake of Election 2000 and Bush v. Gore*, 54 DEPAUL L. REV. 111, 134–35 (2004).

⁷⁰ See *Reynolds*, 377 U.S. at 561.

⁷¹ *Id.* at 536–37.

⁷² *Id.* at 561–62.

Welfare or Spending Clause).⁷³ The Supreme Court has interpreted the Spending Clause to mean that Congress can provide funds to a state in a conditional manner to encourage state conduct in a particular area.⁷⁴ In *South Dakota v. Dole*,⁷⁵ the Court identified three requirements for Congressional appropriations pursuant to the Welfare Clause: Congress may provide federal funds to encourage state action when (1) the spending provides for the “general welfare” of the people; (2) Congress clearly specifies qualifications for receipt of the federal funding; and (3) the conditions of the funding clearly relate to the intent of the spending.⁷⁶ This Spending Clause and the Supreme Court’s interpretation laid, in part, the foundation for Congressional implementation of HAVA, implemented to establish standards for states in the administration of federal elections.⁷⁷

In *Buckley v. Valeo*,⁷⁸ the Supreme Court upheld the constitutionality of Congressional action to use its spending power “as a means to reform the electoral process.”⁷⁹ Following *Buckley*, the Supreme Court as recently as *Bush v. Gore*⁸⁰ recognized that the federal government has the constitutional authority to exercise regulatory power over state and local administration of federal elections.⁸¹

⁷³ U.S. CONST. art. I, § 8, cl. 1 (“The Congress shall have Power To . . . provide for the . . . general Welfare of the United States . . .”); see also Potter & Viray, *supra* note 31, at 105.

⁷⁴ See *South Dakota v. Dole*, 483 U.S. 203, 206 (1987).

⁷⁵ *Id.*

⁷⁶ *Id.* at 207–08; see also Potter & Viray, *supra* note 31, at 105.

⁷⁷ HAVA, Pub. L. No. 107-252, 116 Stat. 1666 (codified at 42 U.S.C. §§ 15301–545 (2006)) (stating in the preamble that the law was enacted “to establish minimum election administration standards for States and units of local government with responsibility for the administration of Federal elections”).

⁷⁸ *Buckley v. Valeo*, 424 U.S. 1 (1976).

⁷⁹ *Id.* at 90; see also Potter & Viray, *supra* note 31, at 105.

⁸⁰ *Bush v. Gore*, 531 U.S. 98 (2000).

⁸¹ *Id.* at 110. In *Bush*, the Supreme Court re-articulated an equal protection argument protecting the fundamental right to vote:

[T]he right to vote as the legislature has prescribed is fundamental The right to vote is protected in more than the initial allocation of the franchise. Equal protection applies as well as to the manner of its exercise. Having once granted the right to vote on equal terms, the State may not, by arbitrary and disparate treatment, value one person’s vote over that of another.

The constitutional source of authority granted to the federal government to regulate and protect the right to vote in federal elections can be found in at least seven separate places.⁸² Unfortunately, even with constitutional authority, voting as universal suffrage did not occur easily in the United States. The history of America is replete with instances of overt aggressions against distinct vulnerable populations⁸³ precluding their participation in the democratic government. Perhaps none more identifiable with exclusion than the era of slavery, enforced servitude and exclusion from public participation as citizens targeted towards African-Americans.⁸⁴ Initially the Thirteenth Amendment, designed to eliminate and release African-Americans from the horrors of slavery, did not provide the newly freed African-American with suffrage.⁸⁵

Congress enacted three subsequent constitutional amendments which directly impacted the right to vote for citizens. The Fourteenth Amendment to the U.S. Constitution⁸⁶ contains the Equal Protection and Due Process Clauses which provided the

Id. at 104 (paraphrasing omitted).

⁸² These places include U.S. CONST. art. I, § 4, cl. 1 (the Elections Clause); *id.* § 8, cl. 1 (the General Welfare or Spending Clause); *id.* cl. 18 (the Necessary and Proper Clause); *id.* amend. XIV (the Enforcement Clause); *id.* amend. XV (prohibiting denial of the right to vote on the basis of race); *id.* amend. XIX (prohibiting denial based on sex); *id.* amend. XXIV (prohibiting denial based on the payment of a poll tax); *id.* amend. XXVI (providing suffrage to persons eighteen and older); *see* Potter & Viray, *supra* note 31, at 103.

⁸³ Jon Hanson & Kathleen Hanson, *The Blame Frame: Justifying (Racial) Injustice in America*, 41 HARV. C.R.-C.L. L. REV. 413, 431–32 (2006) (“In the eighteenth and nineteenth centuries, the westward expansion of the new nation ‘brought mass destruction to the American Indian population.’ But the legitimating frames remained largely intact under the doctrine of ‘Manifest Destiny,’ which ‘saw the Indian’s decline as an inevitable consequence of his racial and cultural weakness and the white man’s vigor.’ It was ‘our manifest destiny to overspread the continent allotted by Providence for the free development of our . . . multiplying . . .’” (citations omitted)).

⁸⁴ *Id.* at 432 (“During much of the time that Native Americans were being forced out of our young nation, an African slave population was being forced in.”).

⁸⁵ U.S. CONST. amend. XIII, § 1 (“Neither slavery nor involuntary servitude, except as a punishment for crime whereof the party shall have been duly convicted, shall exist within the United States, or any place subject to their jurisdiction.”).

⁸⁶ *Id.* amend. XIV, § 1 (“[N]or shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.”); *id.* § 5 (“The Congress shall have power to enforce, by appropriate legislation, the provisions of this article.”).

main protections for the right to vote.⁸⁷ The Equal Protection Clause grants Congress the power to enforce the right to vote. It elucidates the power of the federal government by legislative and judicial means to enforce the fundamental liberties of citizenship.⁸⁸

The Fifteenth Amendment to the U.S. Constitution⁸⁹ was enacted in 1870 to prohibit state impediments which denied a person the right to vote on the basis of color or race.⁹⁰ The southern states and individuals immediately engaged in acts and assaults which included poll taxes, literacy tests, disqualifications, intimidation, and terrorist acts designed to deprive African Americans of the right to vote.⁹¹ The Nineteenth Amendment⁹² granted suffrage to women after a period of intense civil activity and political pressure in 1924.⁹³

⁸⁷ See ERWIN CHEMERINSKY, CONSTITUTIONAL LAW, PRINCIPLES AND POLICIES 13 (2d ed. 2002) (“The Fourteenth Amendment was enacted in 1868 largely to protect the rights of newly freed slaves and in its most important provisions says that no state can deny any person of equal protection of the laws or of life, liberty, or property without due process of law.”); see also *Crawford v. Marion*, 128 S. Ct. 1610, 1611 (2008) (upholding an Indiana statute requiring government issued photo identification to vote as a sufficient means to justify any limitation imposed on voters); *Bush v. Gore*, 531 U.S. 98, 104–10 (2000) (using an equal protection analysis to protect the fundamental right to vote).

⁸⁸ U.S. CONST. amend. XIV, § 5 (“The Congress shall have power to enforce, by appropriate legislation, the provisions of this article.”).

⁸⁹ *Id.* amend. XV.

⁹⁰ *Id.* (“The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any state on account of race, color, or previous condition of servitude.”).

⁹¹ See TAYLOR BRANCH, AT CANAAN’S EDGE: AMERICA IN THE KING YEARS 1965–68, at 1–22 (2006) (detailing the violent struggles of civil rights workers against state led voting rights suppression which culminated in the passage of the 1965 Voting Rights Act); DAVID BRION DAVIS, INHUMAN BONDAGE, THE RISE AND FALL OF SLAVERY IN THE NEW WORLD 327 (2006) (“The tragic collapse of America’s postwar Reconstruction, which the racist North never seriously supported, led in the South to a long era of Jim Crow discrimination that relied, like slavery, on the fear and terror of institutionalized physical violence.”); Bass, *supra* note 69, at 116 (“In direct response to the post-Civil War amendments, the South enacted a number of ‘legal and extralegal’ reforms to limit the political power of freed black men and to enable the Southern caste system to continue. Strategic tools were employed . . . district gerrymandering, purposeful closing of black polling places, poll taxes, literacy tests, grandfather clauses, and above all else, waves of Ku Klux Klan terrorism in the form of lynchings and vigilante violence against blacks and white civil rights activists in the South.”).

⁹² U.S. CONST. amend. XIX.

⁹³ *Id.* “The Constitution as originally drafted and ratified had no provisions ensuring equal protection of the laws. This, of course, is not surprising for a document written for

This era, when coupled with the overt hostility towards American (Native) Indians and the removal of and land acquisition from native Latinos in the early settlement of the Southwest, reflects a period of racial animus, in conflict with the democratic principles of inclusion and equality.⁹⁴ Consequently, the civil rights movement, emergent in the 1940s, identified as one of its principle goals the pursuit of the right to vote for all citizens, with the attendant democratic attributes of inclusion, access and equality.⁹⁵

a society where blacks were enslaved and where women were routinely discriminated against.” CHEMERINSKY, *supra* note 87, at 642. “The Nineteenth Amendment, adopted in 1920, extended the right to vote to women and says that the ‘right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of sex.’” *Id.* at 842.

⁹⁴ Juan F. Perea, *A Brief History of Race and the U.S-Mexican Border: Tracing the Trajectories of Conquest*, 51 UCLA L. REV. 283, 283 (2003) (“The conquest of Mexico between 1846 and 1848 has largely disappeared from public consciousness as a significant historical event with contemporary consequences. Yet this conquest resulted in the annexation by the United States of approximately one-half of former Mexico, constituting most of the current southwestern United States.”). Perea further asserts:

Anglo-Americans together with Mexican Tejans fought a war of independence from Mexico in 1835. Stephen Austin [Texan patriot] described the war in racial terms: “A war of extermination is raging in Texas—a war of barbarism and despotic principles, waged by the mongrel Spanish-Indian and negro race against civilization and the Anglo-American race.”

Id. at 290 (citations omitted); *see also* SALTMAN, *supra* note 7, at 66.

⁹⁵ *See* SALTMAN, *supra* note 7, at 137 (“An initiating factor [for the passage of the Voting Rights Amendment] was the heightened demand on the part of the black community of the South that their second-class citizenship be brought to an end [known as the civil rights movement] The problem of African Americans in the South was not only their inability to vote; it was the pervasive segregation that resulted in inferior treatment in almost every aspect of life.”).

During the civil rights era,⁹⁶ marked by sweeping civil disobedience and major pressure from civil rights activists, the Voting Rights Act of 1965 (“VRA”) was passed.⁹⁷ The VRA addressed discriminatory election practices aimed at the exclusion of racial groups from the voting process.⁹⁸ “The VRA and subsequent amendments established minority voting rights and protections against discrimination on the basis of race, language or color.”⁹⁹

North American voting rights jurisprudence has a long and storied history. From elucidating an articulated “right to vote” to

⁹⁶ *Id.* (describing a nationwide effort to obtain “civil rights” for all citizens irrespective of race, color, creed or nationality).

It is not possible . . . to graphically detail the events of the 1950s and 1960s that led to the passage of the Civil Rights Act of 1964 . . . and the Voting Rights Act of 1965 Despite the Supreme Court ruling in *Brown v. Board of Education of Topeka* in 1954 that school segregation was inherently unequal, little had changed in the years immediately afterward. The Birmingham, Alabama, bus boycott, triggered by Rosa Park’s refusal to give up her seat to a white man, had occurred in 1955. The following years were filled with demonstrations—“sit ins” that attempted to desegregate restaurants and restrooms, demands for “try on” privileges in clothing stores, and violent reactions by some whites. Some blacks who had attempted to register to vote were summarily dismissed, others were shot down . . .

Id.

⁹⁷ Voting Rights Act of 1965 (“VRA”), Pub. L. No. 89-110, 79 Stat. 437 (codified as amended in scattered sections of 42 U.S.C.); *see also* Potter & Viray, *supra* note 31, at 108 (“The VRA and subsequent amendments established minority voting rights and protections against discrimination on the basis of race, language, or color. It abolished the use of literacy tests, ‘good character’ vouchers, and voter requirements impeding the right to vote, and it granted language minorities the right to register and vote in their own languages. The VRA also enabled voters to challenge discriminatory voting practices.” (citations omitted)).

⁹⁸ SALTMAN, *supra* note 7, at 137 (“While the Civil Rights and Voting Rights Acts were intended to end the unconscionable discrimination against African Americans, the elimination of voting restrictions due to race would apply also to American Indians, Alaskan Natives, and Asian Americans.”).

⁹⁹ Potter & Viray, *supra* note 31, at 108 (citing 42 U.S.C. § 1973); *see* SALTMAN, *supra* note 7, at 141 (“The original Act of 1965 was prefaced with the explanation that it was ‘An Act to enforce the 15th Amendment to the constitution of the United States, and for other purposes.’”). The Supreme Court upheld the constitutionality of the Voting Rights Act in *South Carolina v. Katzenbach*, 383 U.S. 301 (1966). *See* SALTMAN, *supra* note 7, at 143.

prohibiting unconstitutional state action, the federal courts ultimately forged a protectionist stance towards voting as a fundamental right and individual liberty.¹⁰⁰ In the twentieth century, impediments or restrictions on voting rights by a state were subjected to strict scrutiny and review by the federal courts. Routine election disputes, however, were subjected to a balancing test with a sliding scale of review required by the courts.¹⁰¹ State election administration and efficiency were considered to be the province of the individual states where very little federal intervention occurred.¹⁰²

In 2000, a controversial presidential election would change all of that, bringing the federal government into a statewide election.¹⁰³ The controversial *Bush v. Gore*¹⁰⁴ ruling was the result

¹⁰⁰ CHEMERINSKY, *supra* note 87, at 842 (“In addition . . . the Supreme Court repeatedly has declared that the right to vote is a fundamental right protected under equal protection Thus it is clearly established that laws infringing on the right to vote must meet strict scrutiny.”).

¹⁰¹ See *Burdick v. Takushi*, 504 U.S. 428, 434 (1992), for a less strict balancing test for voting restrictions imposed by a state where the restrictions are not onerous and the state has a legitimate interest in the regulation thereof. *Burdick*

requires courts to conduct a threshold balancing of the challenged law’s burden on voters against the importance of the purported state interest at stake: if the burden is heavy and the state interest slight, the law is reviewed under the . . . standard of strict scrutiny . . . while if the burden is slight and the state interest significant, the law is examined under the easily met rational basis standard.

Id.; see also *Harper v. Va. Bd. of Elections*, 383 U.S. 663, 670 (1966) (holding that Virginia’s poll tax was unconstitutional as inconsistent with the Equal Protection Clause).

¹⁰² See Bass, *supra* note 69, at 138. Bass analyzed the level of scrutiny applied to such cases:

Arguably, the level of scrutiny in federal voting rights cases should be strict because of the fundamental interest involved. However, with the current Supreme Court ever-watchful of federalism, it has waffled on the scrutiny applied to more nuanced voting rights cases, thus making it difficult to draw a line between when strict scrutiny is triggered and when some lesser level of scrutiny is sufficient.

Id.; see Demian A. Ordway, *Disenfranchisement and the Constitution: Finding a Standard that Works*, 82 N.Y.U. L. REV. 1174, 1177 (2007) (“*Burdick* emphasized voting as an individually held right and proceeded to evaluate whether that right was burdened by the state law.” (citing *Burdick*, 504 U.S. at 434)).

¹⁰³ See Bass, *supra* note 69, at 137 (“The level of scrutiny applicable to Voting Rights Act claims, in light of *Bush v. Gore*, focuses on the remedial avenues available to citizens whose right to franchise has been abridged. The expansive view of voting in *Bush* has opened a window of possibility. The Court opened the opportunity by applying a novel

of a close presidential race in 2000 between Vice-President Albert Arnold Gore, Jr. and Texas Governor George W. Bush.¹⁰⁵ The election was held on November 7, 2000.¹⁰⁶ The next day, Bush was reported to have been the winner.¹⁰⁷ The difference in Florida votes between Bush and Gore was less than one percent.¹⁰⁸ With less than one half of a percent of the vote separating the candidates, Florida law provided for a recount.¹⁰⁹ Gore asked for the recount in four counties.¹¹⁰ However, the Florida Secretary of State refused to extend the deadline for the recount past November 14, 2001.¹¹¹

The election was certified on November 26, 2000, naming Bush the winner.¹¹² Gore filed a contest under Florida law that a state court denied and dismissed.¹¹³ The Florida Supreme Court reversed in part, ordering a manual recount in all counties where a recount had not been held.¹¹⁴

equal protection analysis, with no legal precedent, to the fairness in a state's mechanisms and procedures of the fundamental right to vote."); Carrier, *supra* note 3, at 646. See Paul Charton, *Frying Pan or Fire: Legal Fallout from the Contested 2000 Presidential Election*, 29 U. ARK. LITTLE ROCK L. REV. 669, 669 n.1 (2007) for a summary of books and articles describing the 2000 presidential election including: BRUCE A. ACKERMAN, *BUSH V. GORE: THE QUESTION OF LEGITIMACY* (2002); RICHARD A. POSNER, *BREAKING THE DEADLOCK: THE 2000 ELECTION, THE CONSTITUTION, AND THE COURTS* (2001); Erwin Chemerinsky, *How Should We Think About Bush v. Gore*, 34 LOY. U. CHI. L.J. 1 (2002); Nelson Lund, *The Unbearable Rightness of Bush v. Gore*, 23 CARDOZO L. REV. 1219 (2002); Laurence H. Tribe, *Erog v. Hsub and its Disguises: Freeing Bush v. Gore from Its Hall of Mirrors*, 115 HARV. L. REV. 170 (2001). See also National Archives and Records Administration, 2000 Presidential Election: Popular Vote Totals, http://www.archives.gov/federal-register/electoral-college/2000/popular_vote.html (last visited Mar. 3, 2009).

¹⁰⁴ Bush v. Gore, 531 U.S. 98 (2000).

¹⁰⁵ Bass, *supra* note 69, at 126.

¹⁰⁶ CHEMERINSKY, *supra* note 87, at 860.

¹⁰⁷ *Id.*

¹⁰⁸ *Id.* ("On November 8, the Florida Division of Elections reported that Bush had received 2,909,135 votes and Gore had received 2,907,351 votes.")

¹⁰⁹ *Id.* (citing FLA. STAT. § 102.141(4) (2000)).

¹¹⁰ *Id.*

¹¹¹ See Bush v. Gore, 531 U.S. 98, 101 (2000).

¹¹² *Id.*

¹¹³ *Id.*

¹¹⁴ Richard L. Hasen, *After the Storm: The Uses, Normative Implications, and Unintended Consequences of Voting Reform Research in Post-Bush v. Gore Equal Protection Challenges*, in *RETHINKING THE VOTE: THE POLITICS AND PROSPECTS OF*

The Florida Supreme Court remanded the matter to the trial court.¹¹⁵ A second trial judge ordered the manual recounts to begin.¹¹⁶ Bush filed a petition for a writ of certiorari and a stay in the U.S. Supreme Court.¹¹⁷ The recounts were underway when the Supreme Court stayed the Florida Supreme Court's order, suspended the recount and decided to hear the Florida controversy.¹¹⁸ The parties had effectively turned an election dispute occurring within a state into a matter for the federal judiciary to resolve.¹¹⁹

As the presidency hung in the balance, the Supreme Court granted certiorari to answer questions of law regarding the constitutional issues raised by the Florida election crisis. . . . [including] “[w]hether the Florida Supreme Court established new standards for resolving Presidential election contests, thereby violating Art. II, § 1, cl. 2, of the United States Constitution and failing to comply with 3 U.S.C. § 5, and whether the standardless manual recounts violates the Equal Protection and Due Process Clauses.”¹²⁰

The Supreme Court held that the recount mechanism utilized by the Florida Supreme Court failed and “[did] not satisfy the minimum requirement for nonarbitrary treatment of voters necessary to secure the fundamental right” to vote pursuant to the Equal Protection Clause.¹²¹ The Supreme Court utilized an equal protection standard by stating that “the right to vote as the legislature has prescribed is fundamental; and one source of its fundamental nature lies in the equal weight accorded to each vote and the equal dignity owed to each voter.”¹²² Despite later

AMERICAN ELECTION REFORM 185, 190 (Ann N. Crigler, Marion R. Just & Edward J. McCaffery eds. 2004).

¹¹⁵ *Id.*

¹¹⁶ *Id.*

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ See Tokaji, *supra* note 2, at 1725.

¹²⁰ Bass, *supra* note 69, at 130–31 (quoting *Bush v. Gore*, 531 U.S. 98, 103 (2000)).

¹²¹ *Bush*, 531 U.S. at 105. See Hasen, *supra* note 114, for a recap of the 2000 presidential election disputes.

¹²² *Bush*, 531 U.S. at 104.

vociferous criticism of the Court's reasoning,¹²³ the Court used an equal protection platform to expand oversight of the electoral process, and held that whenever a particular voting procedure effectively "value[s] one person's vote over that of another" there appears to be a plausible claim for an equal protection violation.¹²⁴ It remains to be seen whether the Supreme Court has articulated a new equal protection analysis for garden-variety election disputes.¹²⁵ At first blush, it would appear that in *Bush v. Gore* the Supreme Court mandated the use of the equal protection strict scrutiny test for voting claims as opposed to the balancing test outlined in *Burdick v. Takusi*.¹²⁶

Although it is difficult to predict whether the Supreme Court will continue to analyze voting disputes using the strict scrutiny test, a recent case seems to indicate that the Court will use the balancing analysis in assessing burdens on the right to vote. In *Crawford v. Marion*,¹²⁷ an equal protection challenge to a voter identification law that required voters to show proof of eligibility to register and to vote, the Supreme Court went back to a balancing test analysis.¹²⁸ In *Crawford* the Supreme Court reaffirmed the balancing approach initially outlined in *Anderson v. Celebrezze*¹²⁹:

In *Anderson v. Celebrezze* . . . we confirmed the general rule that "evenhanded restrictions that protect the integrity and reliability of the electoral

¹²³ See Erwin Chemerinsky, *How Should We Think About Bush v. Gore*, 34 LOY. U. CHI. L.J. 1, 5 (2002).

¹²⁴ *Bush*, 531 U.S. at 104–05.

¹²⁵ Hasen, *supra* note 114, at 191–93.

¹²⁶ *Burdick v. Takushi*, 504 U.S. 428, 433–34 (1992). *Burdick* calls for "application of a deferential, 'important regulatory interests' standard for nonsevere, nondiscriminatory restrictions, reserving strict scrutiny for laws that severely restrict the right to vote." *Crawford v. Marion*, 128 S. Ct. 1610, 1624 (2008) (Scalia, J., concurring). *Burdick* requires the courts to use a balancing test which requires the courts to conduct a threshold balancing analysis of the challenged law's burden on the voters against the importance of the state's interest. *Burdick*, 504 U.S. at 434; *see also supra* note 101.

¹²⁷ *Crawford*, 128 S. Ct. 1610.

¹²⁸ In *Crawford* the Court held that the states' interests in deterring and detecting voter fraud, and participating in an effort to modernize election procedures and safeguard voter confidence were sufficiently weighty to justify under an equal protection standard any limitation (such as requiring voters to produce government issued IDs) imposed on the voters. *Id.* at 1617–19.

¹²⁹ *Anderson v. Celebrezze*, 460 U.S. 780 (1983).

process itself” are not invidious and satisfy the standard set forth in *Harper* [v. Virginia Board of Elections]. Rather than applying any “litmus test” that would neatly separate valid from invalid restrictions, [in *Anderson*] we concluded that a court must identify and evaluate the interests put forward by the State as justifications for the burden imposed by its rule, and then make the “hard judgment” that our adversary system demands.¹³⁰

In *Bush v. Gore*, the Supreme Court did not rule on whether the use of inaccurate voting equipment violated equal protection. The Court did identify the technology used in the voting process as an issue for legislative bodies to examine for improvement.¹³¹

As the 2000 presidential election drama played out in Florida, clamors for Congress to take action arose. *Bush v. Gore* may not be the precedent-setting case which resurrected judicial review of strict scrutiny for all state action concerning voting rights.¹³² However, the 2000 controversial presidential election and its judicial progeny—*Bush v. Gore*—were catalysts for HAVA, which mandated improved technology for the states handling federal elections. HAVA also provided the monies for upgrading voting systems that fueled the current voting machine vendor oligopoly.

III. HAVA AND THE PROVISION OF FUNDS

Nearly thirty-seven years after the passage of the VRA, and against the backdrop of the controversial 2000 presidential elections, Congress passed HAVA in November 2002. The Act was designed to incentivize states to improve election-system

¹³⁰ *Crawford*, 128 S. Ct. at 1616 (citing *Harper v. Va. Bd. of Elections*, 383 U.S. 663 (1966) and *Anderson*, 460 U.S. 780).

¹³¹ Tokaji, *supra* note 2, at 1725 (“What is significant about the opinion, for purposes of understanding the subsequent changes in voting technology, is its recognition that the election exposed a serious but previously overlooked problem in need of attention.”).

¹³² Hasen, *supra* note 114, at 191–93.

standards,¹³³ by encouraging states to upgrade their voting systems.¹³⁴ The Act:

- Authorizes \$650 million to purchase punch card voting machines from the states;
- Creates an Election Assistance Commission to serve as a national clearinghouse for information and review of procedures for federal elections;
- Allocates \$3.86 billion in election fund payments to the states over four years to help finance a variety of election improvement projects;
- Establishes minimum standards for state election systems and directs the Department of Justice to monitor and enforce these standards;
- Creates the Help America Vote Foundation and College Program to encourage college students to assist in the administration of state and local elections;
- Mandates provisional ballots by 2004 and statewide computerized voter database by 2006; and
- Reduces postage rates for official election mail.¹³⁵

HAVA as a guideline for selecting the most reliable electronic voting machines for federal elections was and remains woefully

¹³³ HAVA, Pub. L. No. 107-252, 116 Stat. 1666 (codified at 42 U.S.C. §§ 15301–545 (2006)); *see also* Carrier, *supra* note 3, at 646 (“The 2000 presidential election had a searing effect on this nation. Few who witnessed the events in Florida could displace the images of election officials peering at punch cards, struggling to determine the intent of voters. Congress, for example, did not forget. Congress did not wish to see the scenes from Florida replayed in future elections. And so, in 2002, it enacted the Help America Vote Act, known as ‘HAVA’”); Potter & Viray, *supra* note 31, at 110; Steven Ramirez & Aliza Organick, *Taking Voting Rights Seriously: Race and the Integrity of Democracy in America*, 27 N. ILL. U. L. REV. 427, 435 (2007) (“[HAVA] was passed as a response to the controversies surrounding the presidential election of 2000.”).

¹³⁴ Lillie Coney, *A Call for Election Reform*, 7 J. L. & SOC. CHALLENGES 183, 184–85 (2005).

¹³⁵ Hasen, *supra* note 114, at 110.

inadequate.¹³⁶ Although HAVA “provides substantial funding to upgrade voting technology and make other improvements in voting systems,” it unfortunately “provides [only] limited guidance on what type of voting equipment should be implemented, with few binding mandates.”¹³⁷

Significantly, HAVA provides few protections for voting rights against tampering, mistakes and frauds which could occur on an electronic voting machine with copyright and trade secret-protected proprietary software.¹³⁸ The Act does not require verified voter paper trails to ensure against hacking or computer malfunctions.¹³⁹

HAVA established the Election Assistance Commission (“EAC”) without granting any enforcement or regulatory powers.¹⁴⁰ The EAC has no power to issue any rules and

¹³⁶ Ramirez & Organick, *supra* note 133, at 435 (“In general ‘HAVA provided money and imposed some very general standards, while leaving most of the details of election administration to the states and counties.’ In other words, ‘Congress effectively punted.’ . . . HAVA also appears to attempt to resolve issues of auditability. . . . Specifically, the Act requires that the voting system produce a record of audit capacity. In addition, HAVA mandates a ‘permanent paper record’ but provides no clarification to states as to what that ‘permanent paper record’ should record. Nor is there a definition of what is being audited.”).

¹³⁷ Tokaji, *supra* note 2, at 1734.

¹³⁸ See SALTMAN, *supra* note 7, at 196.

This groundbreaking Act of Congress (Public Law 107-252, October 29, 2002) was adopted almost two years after the 2000 general election. The Act has been called ‘an anemic piece of legislation’ . . . but, considering the situation beforehand, it was a giant step forward. . . . Establishment of the Election Assistance Commission (EAC) was a core decision of the act

Id. Saltman contends that the Commission has limited authority and no regulatory enforcement powers. *Id.* at 196–97.

¹³⁹ See Ramirez & Organick, *supra* note 133, at 437 (calling the failure to address this shortcoming of HAVA “a ticking time bomb”); *supra* text accompanying notes 50–52.

¹⁴⁰ See Ramirez & Organick, *supra* note 133, at 437 (“Nor can the EAC [Commission] remedy this confounding statute. Instead, HAVA strips the EAC of any regulatory power; it is a mere funding authority and advisory commission. The Act specifies that the EAC shall not have any new governmental power to ‘issue any rule, promulgate any regulation, or take any other action which imposes any requirement on any State or unit of local government.’”). The EAC can only promulgate advisory standards concerning DREs and software security. *Id.* at 436; see SALTMAN, *supra* note 7, at 196 (“Establishment of the Election Assistance Commission (EAC) was a core decision of the act. . . . The commission has no federal regulatory authority . . .”).

regulations, or to take any actions which impose requirements on any State.¹⁴¹

There are no mandatory basic encryption standards for the transmission of votes or the use of vote recording equipment in HAVA.¹⁴² Nor are there any regulatory provisions requiring software owners to allow access to their proprietary software for independent testing or auditing by citizens, or non-governmental entities.¹⁴³ With increased funding for upgrades to voting procedures, states have adopted and implemented the use of DREs in large numbers. Unfortunately HAVA—the only federal legislation designed to regulate DREs—fails to provide basic protections for the public’s right to transparency and security in the electronic voting process.¹⁴⁴

HAVA was designed to encourage a state to improve its election system standards and thereby encourage the use of electronic voting machines.¹⁴⁵ HAVA funneled money to states to purchase and use electronic voting machines.¹⁴⁶ Yet HAVA fails to adequately provide needed protections required for the efficient provision of this public good—accuracy, transparency and security

¹⁴¹ Ramirez & Organick, *supra* note 134, at 437.

¹⁴² See HAVA, Pub. L. No. 107-252, 116 Stat. 1666 (codified at 42 U.S.C. §§ 15301–545 (2006)).

¹⁴³ See *id.*

¹⁴⁴ See William A. Wright, Comment, *Public Access to Vote-Counting Software*, 1995 U. CHI. LEGAL F. 547 (1995) (providing a discussion on the technology of vote counting software). Wright argues that the current and “suggested security provisions” in vote-counting software do not adequately assure accurate and fair vote counting and that they are not consistent with a public policy of access to vote counting software. *Id.* at 548; see also Cihak, *supra* note 8, at 685 (“As the 2006 election year cycle unfolded, it became increasingly clear that in addition to problems with the installation of new electronic voting equipment, there were other difficulties which plagued the implementation of two more key state HAVA provisions: procedures for the administration of elections and issues dealing with voting accessibility for several population groups.”).

¹⁴⁵ See HAVA, Pub. L. No. 107-252, 116 Stat. 1666; Hasen, *supra* note 114, at 110; see also Philips, *supra* note 7, at 1156.

¹⁴⁶ Philips, *supra* note 7, at 1156 (“HAVA mandates that each state receiving federal funds for the improvement of its federal voting systems replace all ‘punch card voting systems or lever voting systems’ prior to January 1, 2006. This means that optical scan and DRE voting machines will be virtually universally utilized in federal elections beginning in 2006. Included in HAVA are mandatory ‘voting systems standards’ that states must follow for voting machines used in federal elections. . . .”).

in elections using electronic voting technology.¹⁴⁷ HAVA lacks provisions for: (1) a verified voter paper trail; (2) source code disclosures for adequate security testing; (3) encryption measures; and (4) mandatory standards.¹⁴⁸ A recently proposed amendment calls for a verified voter paper trail but fails to require source code disclosures or encryption measures.¹⁴⁹

Coupling the above circumstances with the presence of only a small number of vendors for the entire field of manufacturers creates a problematic paradigm. An oligopolistic industry for DREs was fueled by the infusion of monies from the federal government under HAVA.

Existing voting rights laws were not crafted to protect the public's interest in security and transparency in the digital age of computer voting. The voting legislative history focused on issues of equality and inclusion with very little attention directed toward security and transparency of the voting process.¹⁵⁰ The enactment of HAVA set off a clash between emergent digital technology and voting rights. At this point, voting rights are losing the battle.

IV. INTELLECTUAL PROPERTY RIGHTS: COPYRIGHTS—FEDERAL PROTECTION FOR A PROPERTY INTEREST

The United States Constitution, Article I, Section 8, Clause 8, protects patents and copyrights, as part of the intellectual property regime in this country,¹⁵¹ by providing that Congress shall have the power “to promote the Progress of Science and useful Arts by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.”¹⁵² Unlike the

¹⁴⁷ See sources cited *supra* notes 7 & 144.

¹⁴⁸ See HAVA, Pub. L. No. 107-252, 116 Stat. 1666.

¹⁴⁹ H.R. REP. No. 110-154, at 13 (2007).

¹⁵⁰ See VRA, Pub. L. No. 89-110, 79 Stat. 437 (codified as amended in scattered sections of 42 U.S.C.).

¹⁵¹ See MCCARTHY, *supra* note 44, at 308 (“Certain creations of the human mind [are] given the legal aspects of a property right . . . [i]ntellectual property is an all encompassing term now widely used to designate as a group all of the following fields of law: patent, trademark, unfair competition, copyright, trade secret, moral rights, and right of publicity.”).

¹⁵² U.S. CONST. art. I, § 8, cl. 8.

“right to vote,” intellectual property protections were articulated in the Constitution from the outset as individual property rights.¹⁵³ The Constitution and its iteration of “useful Arts” identify the commercial thrust of this legislation and its utilitarian nature.¹⁵⁴ Intellectual property rights were embedded in the Constitution with a “limited time” to provide incentives for innovation.¹⁵⁵

Based on this constitutional grant of authority, Congress enacted copyright protective legislation in the Act of 1790.¹⁵⁶ Copyrights, a federally protected right granted to fixed, original works of authorship, confer the exclusive right to exploit the work in specified ways for a limited period of time and have been protected by federal statutes since the 18th century.¹⁵⁷ Following the Act of 1790, copyright law was expanded to include musical compositions¹⁵⁸ as well as additional federal jurisdiction to determine copyright matters¹⁵⁹ with Congress ultimately implementing the Copyright Act of 1909.¹⁶⁰

¹⁵³ *Id.*; Copyright Act of 1909, Pub. L. No. 60-349, ch. 320, 35 Stat. 1075 (superseded by Copyright Act of 1976 and amendments); Act of March 3, 1891, ch. 565, 26 Stat. 1106 (The Chase Act) (extending copyright protection to foreign nationals and imposing copyright registration formalities); Copyright Act of May 31, 1790, ch. 15, 1 Stat. 124; SUSAN K. SELL, PRIVATE POWER, PUBLIC LAW: THE GLOBALIZATION OF INTELLECTUAL PROPERTY RIGHTS 60–61 (Cambridge University Press 2003).

¹⁵⁴ *See* SELL, *supra* note 153, at 60–61 (“The emphasis on ‘useful Arts’ underscores the commercial intent of the legislation and the utilitarian rationale behind it. IP rights were devised to create incentives for innovation and risk-taking.”).

¹⁵⁵ *See id.* at 61.

¹⁵⁶ *See* Copyright Act of May 31, 1790, ch. 15, 1 Stat. 124.

¹⁵⁷ *See id.*; SELL, *supra* note 153, at 61 (“The United States passed its first Copyright Act in 1790, which gave citizens and residents a copyright for fourteen years, renewable for an additional fourteen if the author was still alive.”).

¹⁵⁸ *See* *White-Smith Music Publ. Co. v. Apollo Co.*, 209 U.S. 1, 14 (1908) (discussing copyright infringement of musical compositions). *White-Smith* involved the use of perforated music rolls and whether their use constituted an infringement of musical compositions. *Id.* at 15. “Musical compositions have been the subject of copyright protection since the statute of February 3, 1831, ch.16, 4 Stat. 436, and laws have been passed including them since that time.” *Id.* at 26–27. In *White-Smith*, the Court held that the rolls did not constitute copying. *Id.* at 31–32.

¹⁵⁹ Act of Feb. 15, 1819, 15th Cong., 2d Sess., 3 Stat. 481; *see* WILLIAM PATRY, COPYRIGHT LAW AND PRACTICE, VOL. 1, at 38 (1994) (noting the federal courts were not granted original jurisdiction over copyright cases until 1819).

¹⁶⁰ Copyright Act of 1909, Pub. L. No. 60-349, ch. 320, 35 Stat. 1075 (superseded by Copyright Act of 1976 and amendments).

Originally extended to maps and charts in the 18th century,¹⁶¹ today copyright protection can subsist within a novel, play or even a musical score,¹⁶² granting the author protection from unauthorized copying, reproduction or appropriation for original works.¹⁶³

The Copyright Act of 1976,¹⁶⁴ in a sweeping legislative overhaul, established broad categories of copyrightable subject matter.¹⁶⁵ However, the question as to whether copyright protection existed in computer software was not completely resolved by the Copyright Act of 1976.¹⁶⁶

Some scholars argue that a pattern of change has occurred in copyright law which favors the interests of private stakeholders.¹⁶⁷ They contend that the content specific language of newer copyright

¹⁶¹ The Copyright Act of May 31, 1790 provided protection for the author or her assigns of maps, charts, and books for two fourteen year terms, an original and a renewal term.

¹⁶² 17 U.S.C. § 102(a) (2006). Copyrightable subject matter has been divided into eight categories: (1) literary works; (2) musical works; (3) dramatic works; (4) pantomimes and (5) choreographic works; (6) pictorial, graphic and sculptural works; (7) motion picture and (8) audiovisual works. *Id.* Novels are covered under *id.* § 102(a)(1), plays are covered under *id.* § 102(a)(3) and musical scores are covered under *id.* § 102(a)(2). *See* Long, *supra* note 29, at 533 n.34 (“Thus federal copyright protection in the United States has expanded from the narrow categories of protection of charts, maps and books . . . to include photography, motion pictures and computer software.”).

¹⁶³ 17 U.S.C. § 102 (“Copyright protection subsists . . . in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.”); *see* Copyright Act of May 31, 1790, ch. 15, 1 Stat. 124; *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240 (3d Cir. 1983).

¹⁶⁴ Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541 (codified as amended at 17 U.S.C. §§ 101–1332 (2006)).

¹⁶⁵ *See supra* note 162.

¹⁶⁶ *See* I.T. Hardy, *Six Copyright Theories for the Protection of Computer Object Programs*, 26 *Ariz. L. Rev.* 845, 847 (1984) (“Source programs are unquestionably protected by copyright; the rub comes with object programs. The first problem with object programs is determining what they are in the terms of the 1976 Copyright Act.”); Robert A. Kreiss, Comment, *Section 117 of the Copyright Act*, 1991 *B.Y.U. L. Rev.* 1497, 1511 (1991) (“To achieve the proper balance, CONTU recommended two principal changes in the 1976 Copyright Act. The first change was designed to assure computer programmers that computer programs could be copyrighted and that duplicates of a program on disks or tape would be considered ‘copies’ for purposes of copyright infringement.”).

¹⁶⁷ *See* SELL, *supra* note 153, at 63.

laws renders it inflexible and incapable of adapting to technological change. As a result, whenever new technology appears, the law fails to accommodate the change.¹⁶⁸ Then the private stakeholders push for broader legislation, narrowly tailored, designed to give the copyright owners broader and greater rights.¹⁶⁹ Such laws they argue operate to the detriment of the public, the original beneficiaries of copyright law.¹⁷⁰

Computer software¹⁷¹ is designed to function in a utilitarian manner.¹⁷² This makes it difficult to define software within an intellectual property regime. Patent and trade secret law were

¹⁶⁸ See Long, *supra* note 29, at 540 (“Given the increasingly rapid development of technology in the Digital Age, the need for Congress to revise legislation to correct oversights and mistakes becomes even more critical. This need should be directly contrasted with the purported ‘need’ to provide special legislation to protect a particular industry.”).

¹⁶⁹ “The Copyright Act has been amended more times than its sister laws—trademarks and patents. Of these amendments, many have been designed to protect particular industries, such as the exemption of computer software and sound recordings from the strictures of the First Sale Doctrine codified in [§] 109 of the Copyright Act.” *Id.* Long opines that such exclusions should have been the exception and should have only occurred to balance copyright privileges and public access when undue prejudice to the copyright exists. See *id.*; see also Robert E. Thomas, *Vanquishing Copyright Pirates and Patent Trolls: The Divergent Evolution of Copyright and Patent Laws*, 43 AM. BUS. L.J. 689, 690 (2006) (The “income-generating value of intellectual property gives intellectual property owners incentives to influence the direction of legislative change in order to maximize intellectual property returns. Highly visible examples of changes that arguably benefited intellectual property owners include time extensions such as the Sonny Bono Copyright Term Extension Act, which protects creative works for as long as 120 years, and the 1995 revisions to the Patent Act, which changed the calculation of patent term to 20 years from filing.”).

¹⁷⁰ SELL, *supra* note 153, at 63. There is a “legislative pattern in United States copyright law of privileging private interests of authors and owners at the expense of the interests of the public in use and reuse of copyrighted information.” Keith Aoki, *(Intellectual) Property and Sovereignty: Notes Toward a Cultural Geography of Authorship*, 48 STAN. L. REV. 1293, 1310 (1996).

¹⁷¹ Software is a “set of computer programs, procedures, and possibly associated documentation concerned with the operation of a data processing system, e.g. compilers, library routines, manuals, circuit diagrams. Contrasts with hardware.” U.S. COPYRIGHT OFFICE, COMPENDIUM II: COPYRIGHT OFFICE PRACTICES § 326 (1984), available at http://ipmall.info/hosted_resources/CopyrightCompendium/fplchome.asp [hereinafter Compendium II]; SCOTT, *supra* note 46, at 741 (“Software”).

¹⁷² See LEMLEY, *supra* note 45, at 33 (“Computer software, by its very nature as written work intended to serve utilitarian purposes, defies easy categorization within our intellectual property system.”).

designed to protect new utilitarian property. Copyright law, on the other hand, was designed to protect original literary works.¹⁷³ The stage was set for an expansion of copyright laws to include emerging computer software technology.¹⁷⁴

Congress established the National Commission on the New Technological Uses of Copyright Works (“CONTU”) in 1978.¹⁷⁵ CONTU’s mission was to study copyright law and its interrelatedness to computer programs.¹⁷⁶ CONTU’s Final Report contained recommendations that were the results of hearings and investigative studies.¹⁷⁷ Congress requested that the Commission study policy questions in the copyright field.¹⁷⁸ One of the problems assigned to the Commission was the question of the scope of extension of copyright protection to computer programs.¹⁷⁹ CONTU’s recommendations were ultimately adopted by Congress as the amendments of the 1980 Act.¹⁸⁰

¹⁷³ See *id.*

¹⁷⁴ See SELL, *supra* note 153, at 63 (“Over time, the scope of subject matter eligible for copyright protection has broadened considerably. For example . . . ‘the major computer lobbyists in the United States pressed for computer programs to be protected by accretion by treating them as literary works within traditional norms of copyright; and they now have persuaded much of the world to adopt this approach.’” (quoting W.R. Cornish, *The International Relations of Intellectual Property*, 52 CAMBRIDGE L.J. 55 (1993)).

¹⁷⁵ FINAL REPORT OF THE NATIONAL COMMISSION ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS (1978), available at <http://digital-law-online.info/CONTU/PDF/index.html> [hereinafter CONTU Final Report].

¹⁷⁶ See Christian H. Nadan, *Software Licensing in the 21st Century: Are Software “Licenses” Really Sales, and How will the Software Industry Respond?*, 32 AIPLA Q. J. 555, 564–65 n.20 (2004) (CONTU was “a congressional commission created to ‘recommend changes in the Copyright Act to accommodate advances in computer technology.’”) (citing *DSC Commc’ns Corp. v. Pulse Communications, Inc.*, 170 F.3d 1354, 1360 (Fed. Cir. 1999)).

¹⁷⁷ See CONTU Final Report, *supra* note 175, at 1.

¹⁷⁸ See *id.*

¹⁷⁹ See *id.* at 1, 9–46.

¹⁸⁰ See H.R. REP. No. 96-1307, sec. 8 (1980), as reprinted in 1980 U.S.C.C.A.N. 6460, 6482 (noting that the 1980 amendments to the Copyright Act were intended to implement CONTU’s recommendations); *Kramer Mfg., v. Andrews*, 783 F.2d 421, 432 n.8 (4th Cir. 1986) (“The [A]mendments of 1980 followed the Final Report of the Commission on New Technological Uses of Copyright[ed] Works (CONTU) . . . [t]he Amendments of 1980 conformed to [CONTU’s] recommendations.”); *Apple Computer, Inc. v. Formula Int’l, Inc.*, 594 F. Supp. 617, 621 (C.D. Cal. 1984) (“[T]he most valuable legislative history materials concerning the Copyright Act of 1976 and the Amendment of 1980 are the reports of CONTU.”).

Unsurprisingly, software was included as a copyrightable subject matter in CONTU's recommendations.¹⁸¹

The 1980 amendment to the Copyright Act, extended copyright subject matter protection to application programs and operating system programs in both object code and source code versions.¹⁸² This amendment opened the door to the current legal conflict which occurs when DREs are used with copyright protected software inaccessible to the public during federal elections.¹⁸³ The inaccessibility of the software for independent review and auditing purposes means that the public cannot ascertain whether hacking, fraud or corruption of the voting process has occurred.¹⁸⁴ Private vendors, owners of protected intellectual property, now exert access control in an area where voting—a public good—exists. The stage is set for a clash.

A. *Source Code and Object Code and Copyright Protection*

In order to operate, DREs use computer operating systems. These systems employ computer programs containing object and source codes. The object¹⁸⁵ and/or source code¹⁸⁶ is usually the

¹⁸¹ See LEMLEY, *supra* note 45, at 35 (“Congress implemented CONTU’s recommendations in 1980 by adding a definition of ‘computer program’ to [§] 101 of the Copyright Act and amending [§] 117 of the Act to authorize the owner of a copy of a computer program to make another copy or adaptation of the program for the purpose of running the program on a computer.”).

¹⁸² Act of December 12, 1980, Pub. L. No. 96-517, 94 Stat. 3015. “‘A copyright program, whether in object code or source code, is a ‘literary work’ and is protected from unauthorized copying, whether from its object source or source code version.’” MCCARTHY, *supra* note 44, at 405 (quoting *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1240 (3d Cir. 1983)).

¹⁸³ Massey, *supra* note 28, at 234 (“The source of this problem is the proprietary source code that drives these paperless electronic voting machines. Unlike paper based voting machines, DREs operate entirely by computer, meaning that at no state of the election process can the public see the physical counting of the votes. Absent access to the source code that the runs the DRE, the public has no way of knowing how—or if—the machine records and tabulates votes.”).

¹⁸⁴ *Id.* at 235.

¹⁸⁵ MCCARTHY, *supra* note 44, at 409 (“Object code is [t]he lowest level of computer language. Object code is ‘machine readable’ by a computer and cannot be read by humans. Object code is often expressed in binary language, using ‘on-off’ or ‘0-1’ notation such as ‘01101001’. Computer programs written in source code are readable by human and are written in computer languages such as BASIC or FORTRAN. However, computers cannot understand source code, so to use the program, it must be translated

property of the vendor owners of the machine and is subject to copyright protection. The purchaser of the machine, typically a governmental entity generally, has limited access to this copyrighted protected material without permission.

The term source code refers to a computer program written in programming language that uses complex symbolic names, along with complex rules of syntax.¹⁸⁷ Some of the languages are BASIC, COBOL or FORTRAN.¹⁸⁸ The purpose of the source code is to provide instructions to the computer to perform a particular task.¹⁸⁹ CONTU also weighed in on the definitions of object code and source code in its final report to Congress.¹⁹⁰

Object Code is most succinctly defined as:

[A] translation of the source code language into the machine language of the computer (e.g. binary coding using zeros and ones or hexadecimal coding using letters and numbers or octal coding using zero to seven) that the computer executes. Only instructions expressed in object code can be used 'directly' by the computer.¹⁹¹

A government or public entity who has purchased a DRE that relies on object and source code, absent cooperation, cannot validate that the code is operating as it should, is not subject to unusual errors or irregularities or contains vulnerabilities which subject the entire process to hacking, subversion or manipulation. The governmental entity has to rely upon the owner or vendor of the machine for assurance that the voting machine will operate, or has operated (after an election), as it should for the purposes of a

into machine-readable object code. Computer programs written in both source code and object code are copyrightable and can qualify as trade secrets."); *see Whelan Assocs. v. Jaslow Dental Lab. Inc.*, 797 F.2d 1222, 1231 (3d Cir. 1986) ("In every program, it is the object code, not the source code, that directs the computer to perform functions. The object code is therefore the final instruction to the computer.").

¹⁸⁶ See *supra* note 46 for a definition of source code.

¹⁸⁷ *Lotus Dev. Corp. v. Paperback Software Int'l*, 740 F. Supp. 37, 44 (1990).

¹⁸⁸ *Compendium II*, *supra* note 171, § 321.01.

¹⁸⁹ See generally RUBIN, *supra* note 7, at 3; Massey, *supra* note 28, at 238.

¹⁹⁰ CONTU Final Report, *supra* note 175, at 21 n.109.

¹⁹¹ SCOTT, *supra* note 46, at 553; see also CONTU Final Report, *supra* note 175, at 21 n.109.

fairly conducted election if the vendor owner disallows access to the software for testing. The voter as the end user of the computer voting machine has even less access to the computer program. The DRE vendor with copyright and trade secret protections for its software does not provide an independent right of review or audit of its property. Thus the voter cannot affirm that his or her right to participate in a fairly conducted election has not been circumvented by faulty or even ineffective computer programs for voting, or recounting purposes.¹⁹²

In addition, the Digital Millennium Copyright Act (“DMCA”),¹⁹³ passed by Congress in 1998, poses problems for voting rights. Originally created as an uneasy solution to the problems of copying on the Internet,¹⁹⁴ the DMCA was designed to eliminate the contributory liability of Internet service providers for the transmission of allegedly infringing works.¹⁹⁵ The DMCA provided safe harbors for Internet service providers who were then obligated to protect the rights of copyright owners after receiving notice of infringement from the copyright holder.¹⁹⁶ The Internet provider had to “take down” the infringing material or suffer the loss of the safe harbor provisions.¹⁹⁷

In addition to the notice and take-down provisions, the DMCA contains subpoena power for the copyright holder.¹⁹⁸ This power allows the copyright holder to procure a subpoena from a federal district clerk to obtain disclosure from the service provider of the identity of a purported infringer.¹⁹⁹ This disclosure provision designed “to protect music from digital pirates” provides a chilling

¹⁹² See Massey, *supra* note 28, at 242–43 (noting that auditing, without access to the proprietary source code, “becomes a pointless endeavor because all an auditor has to work with is potentially flawed election data produced by a black box in which it is impossible to see how it created that data”).

¹⁹³ See Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).

¹⁹⁴ See Long, *supra* note 29, at 533–36.

¹⁹⁵ See *id.* at 536–37.

¹⁹⁶ See *id.* at 537; see also 17 U.S.C. § 512(b)(2)(E) (2006).

¹⁹⁷ See *id.* at 537–38.

¹⁹⁸ *Id.* at 538 n.25 (“Upon receipt of the issued subpoena . . . the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena. . . .” (citing 17 U.S.C. § 512(h)(5))).

¹⁹⁹ *Id.* at 538.

mechanism for software owners to suppress any dissemination of materials concerning proprietary information on voting machines.²⁰⁰

The software developer for voting machines and/or owner typically use both copyright²⁰¹ and trade secrecy protection for their works as proprietary intellectual property, because trade secrecy provides advantages to the vendors in addition to those available under copyright or patent.²⁰² Again the intellectual property protections available to the DRE vendor and its software appear to outweigh the voting rights concern of the public.

V. TRADE SECRETS—STATE INTELLECTUAL PROPERTY PROTECTION

The intellectual property protection which provides more extensive coverage for the software contained in DREs is the commercial tool of trade secrets.²⁰³ State laws generally provide protection for intellectual property as technological information through trade secrets.²⁰⁴ While copyright protection for a product emanates from federal law, trade secret protections generally are

²⁰⁰ *Id.* at 543 (suggesting that DRE vendor Diebold's use of procedures designed to prohibit digital piracy to prohibit the dissemination of information regarding e-voting security highlights the problematic nature of DMCA procedures and the imminent threat to "the free circulation of speech and information").

²⁰¹ *See supra* notes 162–84. Copyright duration is extensive: for works created after 1977, the term is 70 years plus the author's lifetime; for works made for hire, the term is 95 years from first publication or 120 years from the year of creation whichever expires first. 17 U.S.C. § 302.

²⁰² *See Levine, supra* note 7, at 135 ("Trade secrecy—the intellectual property doctrine that allows businesses to keep commercially valuable information secret for a potentially unlimited amount of time—is increasingly intruding in the operation of our public infrastructure, including voting machines, the Internet, and telecommunications.").

²⁰³ *See id.* at 136–37 ("Trade secrecy, by its very name, invokes two core interests: secrecy and commerce. It is a singularly commercial doctrine designed to protect commercial interests by allowing companies and individuals to keep secret, for a potentially unlimited time, those formulas, processes and inventions that afford them pecuniary gain.").

²⁰⁴ *See LEMLEY, supra* note 45, at 4 ("Today, every one of the 50 states protects trade secrets in one form or another.").

derived from state law.²⁰⁵ Initially states relied on the Restatement (First) of Torts:

A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for machine or other device, or a list of customers.²⁰⁶

Trade secret laws, although adopted in a piecemeal fashion from state to state, provide astute vendors with a strong defensive enforcement tool for keeping their proprietary software out of reach of inquiring minds or auditing hands while copyright protection is limited to tangible expressions.²⁰⁷

²⁰⁵ See Levine, *supra* note 7, at 155–56 (“By 2005, a form of the UTSA [Uniform Trade Secret Act] had been adopted in forty-four states and the District of Columbia.”); see also *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 475 (1974) (citing state authority for trade secret protection).

²⁰⁶ RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939); see also Uniform Trade Secrets Act (1939); James Gibson, *Once and Future Copyright*, 81 NOTRE DAME L. REV. 167, 171 (2005) (arguing that the unsuccessful marriage of copyright and technology has created a new legislative regulation of technological behavior, which may be dubbed “technological” regulation).

For example, the legal entitlements of trade secret law reinforce software's technological ability to keep its creative expression from reaching the public. The Digital Millennium Copyright Act [for example] puts its considerable legal weight behind the technological access restrictions and copy protection that copyright owners use to control their digital goods For source code, the more important protection is found in trade secret law, a regulatory regime predicated on maintaining the secrecy of valuable commercial information, such as formulas or manufacturing processes Therefore, as long as a software developer takes reasonable steps to keep source code secret from the prying eyes of competitors and the public, trade secret law provides legal remedies for its unauthorized and improper appropriation.

Id. at 171–72, 177 (paragraphing omitted).

²⁰⁷ 17 U.S.C. § 102(b) (2006) provides that copyright protection does not extend to any “idea, procedure, process, system, method of operation, concept, principle or discovery, regardless of the form in which it is described, explained, illustrated or embodied in such work.” Note, however, that the subject matter of trade secret law is not limited to tangible expression, but allows for protection of an idea that has not been reduced to

Gradually states have adopted The Uniform Trade Secrets Act (“UTSA”) that is now implemented in forty-three different states.²⁰⁸ The UTSA provides a starting point for understanding trade secret law applicable to the technology inherent in DRE voting machines. UTSA defines a trade secret as:

information, including a formula, pattern, compilation, program device, method, technique, or process, that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.²⁰⁹

This broad statutory definition provides the owner of software a viable mechanism for preventing copying, reproduction or access to the inner workings of the intellectual product under the mantle of maintaining trade secret protection.²¹⁰

The Seventh Circuit provided a telling description of the amorphous nature of a trade secret.²¹¹ The concept of trade secrets is a chimerical, unanalyzed concept, which arises as a secondary

tangible form as long as there is sufficient concreteness. *See* UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 437 (1985) (defining a “trade secret” as “information, including a formula, pattern, compilation, device, method, technique, or process”). Thus the astute business person can fashion IP protection for technological concrete “ideas” as well as copyrightable tangible products using a combination of both trade secrets and copyright protection.

²⁰⁸ *See* 1-5 LESTER HORWITZ & ETHAN HORWITZ, INTELLECTUAL PROPERTY COUNSELING AND LITIGATION § 5.01(1) (MB 2008) (“Although the most frequent source of trade secret law was traditionally state common law, since 1980 some 43 states and the District of Columbia have enacted the Uniform Trade Secrets Act.”).

²⁰⁹ UNIF. TRADE SECRETS ACT § 1, 14 U.L.A. 437 (1985).

²¹⁰ RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939). The Minnesota Supreme Court in *Cherne Industries, Inc. v. Grounds & Assoc.* 278 N.W. 2d 81, 90 (Minn. 1979) recited a “workable test” for trade secret in an employee-employer dispute that can be applied generally: “(1) the protected matter is not generally known or readily ascertainable, (2) it provides a demonstrable competitive advantage, (3) it was gained at expense to the employer, and (4) it is such that the employer intended to keep it confidential.” *Id.* at 90.

²¹¹ *Smith v. Dravo Corp.*, 203 F.2d 369, 373 (7th Cir. 1953).

consequence of the primary precept that the law expects everyone to adhere to the rudimentary requirements of good faith.²¹² Almost any type of knowledge or information used in the conduct of business is amenable to being characterized as a trade secret.²¹³

Even prior to the adoption of copyright protection laws for computer software, owners tried to prevent users from copying their software by claiming trade secrecy protection for the programs.²¹⁴ Although not without weaknesses, trade secret protection provides an appropriate defense for software owners and the owners of electronic voting machines to use in protecting their intellectual property. Its chimerical nature allows businesses to place many of their intellectual property assets under the protective arm of a trade secret defense as long as the requirements are met.²¹⁵

The weaknesses of trade secret protection occur because of its very nature.²¹⁶ A trade secret can exist only if its proprietor takes steps to maintain its secrecy and it is substantially a secret within the industry.²¹⁷ Also independent invention and reverse engineering can be used to circumvent trade secret protection.²¹⁸

²¹² E.I. DuPont De Nemours Powder Co. v. Masland, 244 U.S. 100, 102 (1917).

²¹³ *Smith*, 203 F.2d at 373.

²¹⁴ See LEMLEY, *supra* note 45, at 4 (“Against this backdrop, it was important for software vendors in the 1970s and early 1980s to establish the rights vis-a-vis users. One way for vendors to prevent users from freely copying their computer programs was to claim a program as a trade secret.”).

²¹⁵ See HORWITZ & HORWITZ, *supra* note 208, § 5.01(1) (“In making a determination whether information is susceptible to protection as a trade secret, counsel should determine whether it qualifies on each of five points. . . . (1) Appropriate subject matter; (2) Maintained as secret; (3) Not generally known in the industry; (4) Commercialized or of potential value; and (5) Concrete.”).

²¹⁶ *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 490–91 (1974); see Levine, *supra* note 7, at 146–47 n.42 (“Indeed, one of the major differences between trade secrecy law and the other three major areas of intellectual property (trademarks, copyrights, and patents) is that those three areas have significant statutory support and history Thus in order to explore the underpinnings of trade secrecy, it is especially important to review early case law and those opinions that became the classic statements of trade secrecy’s definition, application, and purview.”); see also 15 U.S.C. (codifying trademark law); 17 U.S.C. (2006) (codifying copyright law); 35 U.S.C. (2006) (codifying patent law).

²¹⁷ *Kewanee Oil Co.*, 416 U.S. at 490–91. In order to protect a trade secret the owner must work to render the product as immune as possible to reverse engineering or risk a diminution of exclusivity. *Id.* at 476.

²¹⁸ *Id.* at 476.

In order to maintain trade secret protection, the owners of trade secrets are required to establish stringent secrecy protocols for anyone licensing or using their equipment.²¹⁹

Trade secret protections can be used to prevent election officials from releasing DRE software to independent auditors for a review and testing of the electronic software within DREs.²²⁰ This is particularly important as a second stage check for a security audit.

Simultaneously the term of protection for trade secrets is of an unlimited duration.²²¹ The protection afforded by trade secret law is both greater and less than that given under patent law.²²² Trade secret protection is greater than patent law because it is not limited to a fixed number of years and does not require novelty and invention as in the case of patents. It affords less protection than patent law because other persons can develop the technology independently and use it as long as no unfair or fraudulent means were used.²²³ It does not require the originality of copyright nor fixation. In fact, its strength may lie in the owners' ability to maintain it as knowledge and pure information.

As one scholar phrased it:

[t]he source of this problem [trade secret protection for electronic computer software] is the proprietary source code that drives these paperless electronic voting machines. Unlike paper-based voting machines, DREs operate entirely by computer, meaning that at no stage of the election process can the public see the physical counting of the votes. Absent access to the source code that runs the DRE,

²¹⁹ *Id.* at 486–87.

²²⁰ Long, *supra* note 29, at 551 (“[T]he encryption and security testing exceptions must be expanded to allow for legitimate testing, including by amateurs, of encryption and security devices.”).

²²¹ *Kewanee Oil Co.*, 416 U.S. at 494 (Marshall, J., concurring).

²²² *Id.* at 489–90. Patents are “[a] grant by the federal government to an inventor of the right to exclude others from making, using, or selling the invention.” MCCARTHY, *supra* note 44, at 433. The subject of a patent must be novel, nonobviousness and useful. *Id.* at 435; *see also* 35 U.S.C. §§ 101–02 (2006) (describing what inventions are patentable and conditions for patentability).

²²³ *See supra* note 218.

the public has no way of knowing how—or if—the machine records and tabulates votes.²²⁴

Computer software programs have been afforded intellectual property protection as copyrighted proprietary products and as trade secrets.²²⁵ The intellectual property laws are ostensibly designed to protect the owner's business advantage while encouraging creativity and innovation.²²⁶ Copyright infringement laws provide swift remedial justice to anyone copying or unlawfully acquiring the use of said intellectual property in software.²²⁷ Trade secret protection provides unlimited duration for the intellectual property rights of the owner.²²⁸

The prevailing economic theory on patents and copyrights is that intellectual property protection allows the owner the use and enjoyment of her property for a limited time. At the end of that time, so the theory goes, the information, technology, and knowledge enters the public domain for the use and enjoyment of

²²⁴ Massey, *supra* note 28, at 234.

In practice, proprietary code-based DREs have proven to be error-ridden and prone to security weaknesses because the closed nature of the code has forced state agencies to protect manufacturers' intellectual property at the expense of a reliable voting system. The proprietary nature of the code requires a closed state review process that has not eliminated serious errors and security flaws because it limits the number of people testing the software. That closed process also contradicts public policy and American tradition favoring openness through transparent and accountable government.

Id. at 235.

²²⁵ See *supra* notes 182–84, 214–15; see also David Bender, *The Future of Software Protection: Protection of Computer Programs: The Copyright/Trade Secret Interface*, 47 U. PITT. L. REV. 907, 939 (1986).

²²⁶ SELL, *supra* note 153, at 60–61 (“The United States included intellectual property in the Constitution The emphasis on ‘useful Arts’ underscores the commercial intent of the legislation and the utilitarian rationale behind it. IP rights were devised to create incentives for innovation and risk-taking. This is consistent with both Benthamite and Lockean notions of property: ‘with property rights people have an incentive to labour and industry will prosper.’”); see Levine, *supra* note 7, at 137 (“Trade secrecy, by its very name, invokes two core interests: secrecy and commerce. It is a singularly commercial doctrine designed to protect commercial interests by allowing companies and individuals to keep secret, for a potentially unlimited time, those formulas, processes, and inventions that afford them pecuniary gain.”).

²²⁷ Bender, *supra* note 225, at 912; see Thomas, *supra* note 225, at 709–11.

²²⁸ *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 494 (1974) (Marshall, J., concurring).

the public.²²⁹ The monopoly is created to incentivize innovation ends. The author has been rewarded and the discovery, knowledge and information become part of the public commons.²³⁰

The protections found in trade secrets do not have a parallel theory of replenishing the commons. It is designed entirely for the benefit of the commercial user.²³¹

Some scholars have argued that copyright's reach has also established a commodification of creativity. They argue that the tools of this commodification process have included the alienability of the copyright interest, the long duration of copyright, the strong distribution rights and the demise of significant user rights.²³² This argument posits that the copyright owners' power has expanded vis-à-vis those wishing to use copyright material because of a contraction of user rights, to include fair dealing/fair use rights and public interests rights.²³³ Yet copyright protection does have a limited duration. It was also designed with the competing interests of the public and the property interest of the copyright owner in mind.

In trade secret law, the private stakeholders' interest and the public's clash in the intersection of public rights and commerce. Trade secret law in areas where "private businesses are utilizing commercial law standards and norms, including the key tool of

²²⁹ See Michael Carrier, *Cabining Intellectual Property Through A Property Paradigm*, 54 DUKE L. J. 1, 33 (2004). "Allowing such imitation obviously would deter future innovators and result in a suboptimal level of innovation. To prevent this result, the patent and copyright laws grant inventors a right to exclude." *Id.*

²³⁰ *Id.* at 32.

²³¹ *Id.* at 32–33; see Levine, *supra* note 7, at 136 ("Trade secrecy, by its very name, invokes two core interests: secrecy and commerce. It is a singularly commercial doctrine designed to protect commercial interests by allowing companies and individuals to keep secret, for a potentially unlimited time, those formulas, processes, and inventions that afford them pecuniary gain.").

²³² BIRGITTE ANDERSEN, *INTELLECTUAL PROPERTY RIGHTS: INNOVATION, GOVERNANCE, AND THE INSTITUTIONAL ENVIRONMENT* 46 (2006).

²³³ *Id.* at 48.

This has been accompanied by significant shifts in rhetoric. Not only have the monopoly privileges of intellectual property owners become 'rights', user rights have become 'defenses' or 'exceptions'. The public domain is thus protected by 'exceptions' to rights. Nothing could better encapsulate its current vulnerability.

Id.

trade secrecy,” conflicts with the “methods and purpose of transparent and accountable democratic governance.”²³⁴ Where voting machines are involved the public is expecting a device which furthers governmental and democratic interests²³⁵ not a commercially competitive product.

Recently, the owners of one of the top DRE vendors have admitted that the machines include software flaws.²³⁶ However, without the accessibility of the software for independent audit purposes, the public cannot be assured of security and accountability in the vote process.

With the admixture of copyright and trade secret protection in the voting machines, the DRE software has a potentially unlimited lifetime of protection coupled with strong tools for its enforcement against interference. As a result of this combined protection, the software owner in voting machines can maintain unlimited intellectual property protection duration and the public does not have independent access to the public good. Critically the public is denied access to a fundamental public utility, the election system, during the voting process.²³⁷

²³⁴ Levine, *supra* note 7, at 137–38 (“Secrecy, and its attendant goals of pecuniary gain and commercial competition, conflict with the methods and purpose of transparent and accountable democratic governance. This conflict is crystallized in the private distribution of voting machines.”).

²³⁵ *Id.* at 138 (“These machines, replacing older (but not necessarily less reliable) pull-lever and punch-card systems, are the public infrastructure through which elections are conducted, votes are counted, and the results are verified. They form the backbone upon which one can exercise the right to vote; they instill confidence that one’s vote will not be disregarded, lost, or erroneously tabulated.”).

²³⁶ Ellen Gedalius, *Company Accepts Blame for Vote Woes*, TAMPA TRIBUNE, Aug. 28, 2008, at 1. In the Hillsborough County, Florida primary election in August, Premier Election Solutions accepted responsibility for a glitch in the system that caused a delay in posting the election results. *Id.* “The problem occurred because the identification numbers for the different databases—for absentee, early, and precinct votes—did not match, so the numbers could not be merged into one report.” *Id.* Premier stated that the \$6 million system will work properly in the general election in November. *Id.*; *see also* Duane Marsteller, *Elections Officials Back Machines Despite Reported Glitch*, BRADENTON HERALD, Aug. 23, 2008, at 1. Premier Election Solutions notified counties across the U.S. that their machines have a glitch that causes the actual counting machine to prematurely display a completion screen before all of the votes are uploaded into the system to be tallied. *Id.*

²³⁷ *See* Levine, *supra* note 7, at 140 (asserting that the access to information so necessary for a transparent and accountable democratic government suffers as private

A. *Oligopoly in the DRE Marketplace*

1. The Prisoner's Dilemma and Voting Rights

In this section, this Article proposes to use game theory tools to describe how the DRE oligopoly acts to upset the balance between voting rights and intellectual property rights.²³⁸ Both intellectual property rights and voting rights are constitutionally protected interests.²³⁹ Normally, in the face of a conflict between two protected rights, the competing fundamental interests would be identified and the countervailing interests weighed. In the midst of competing claims, the law would weigh in and survey the contextual background, attempt to impose a balancing of the interests analysis and ultimately prioritize the rights. Unfortunately, in an oligopoly the vendors by collectively controlling the price, the output, and supply²⁴⁰ ultimately upset the balance between the two rights by asserting primacy for the property right over the individual liberty of voting. They do this

industry both increasingly relies on secrecy to maintain its competitive edge and private industry increasingly expands into the provision of public infrastructure and democratic functions such as voting). “[T]rade secrecy law and practices serve many useful and important purposes in private industry, but . . . their use in the public infrastructure is inappropriate, unexpectedly powerful, and doctrinally unsound.” *Id.*

²³⁸ See Piraino, *supra* note 25, at 18–19. The small concentrated market of an oligopoly makes it easier for the firms to collectively set their output and pricing. *See id.*

Recent models of game theory explain why oligopolists are able to maintain a price equilibrium at a level above that which would prevail in a perfectly competitive market (i.e., above marginal cost) . . .

..

....

. . . Each firm recognizes its interdependence with other firms in the market and understands that “its optimal price is a function of the price charged by its rivals.” An oligopolist is aware that its rivals are as strongly armed as it is with weapons of price reductions, aggressive advertising, and product improvement. Thus each firm will want to avoid prompting aggressive competitive responses from its rivals. If one firm cuts prices in an effort to boost sales, rivals may be compelled to match the price cut, not only rendering the initial effort to secure additional volume unsuccessful, but making all firms worse off than before.

Id.

²³⁹ See *supra* note 31 and accompanying text.

²⁴⁰ See *supra* notes 5, 24–25 and accompanying text.

by collectively refusing to allow access to their software for independent auditing and testing and by refusing to upgrade their technology to address security, accuracy and transparency problems. Their conduct as an oligopoly eliminates non-price competition in areas of quality, service and access.

In examining a game called the Prisoner's Dilemma,²⁴¹ we observe how two firms collectively can operate to maintain control and preclude access.²⁴²

Two hypothetical salesmen, Joshua and Jake, were arrested for hacking into a computer system and downloading customers' personal information with the intent to commit identity theft. At the police station, the authorities separated and interrogated them. The police offered the following deal to each one separately: confess or remain silent. If Joshua confessed (implicated Jake) and Jake remained silent, Joshua would receive one year in prison—a short sentence for cooperating with the police and helping to prove charges against Jake. In this scenario, Jake would receive ten years.

If, however, Jake confessed implicating Joshua who remained silent, Jake would receive one year in prison and Joshua would receive ten years. If they both confessed, they would each receive five years for saving authorities from having to prove the charges in trial. If neither confessed, the authorities might be able to sentence them each with six months for unlawful use of computer property, but the authorities would not be able to charge either with identity theft. The best strategy for either Joshua or Jake is to confess, without cooperating with the other.²⁴³

Confessing is the best strategy for Joshua whether or not he knows if Jake is going to confess. It is also the best strategy for Joshua whether or not he knows if Jake is going to remain silent.

²⁴¹ See *supra* note 11 for a discussion of the Prisoner's Dilemma.

²⁴² ROBERT GIBBONS, *GAME THEORY FOR APPLIED ECONOMISTS 4* (Princeton University Press 1992) (1958) (describing the classic tool of game theory called a normal-form representation, where each player simultaneously chooses a strategy, and the combination of strategies chosen by the players determines a payoff for each player); RASMUSEN *supra* note 11, at 21; see also *supra* note 11 (quoting Rasmusen's description of the Prisoner's Dilemma).

²⁴³ See *supra* note 11; see generally RASMUSEN, *supra* note 11, at 19–22.

Joshua does not need to know anything about Jake's strategy to know that the best strategy for him is going to be confession. The same holds true for Jake. Why? Because if Joshua confesses, he will be better off, no matter what Jake does, and the reverse is true for Jake. The game matrix below represents the choices for the two prisoners. Joshua's choices are represented by the first number. Jake's choices are represented by the second number.

	Jake: Deny (protect Joshua)	Jake: Confess (blame Joshua)
Joshua: Deny (protect Jake)	6 mos, 6 mos	10 yrs, 1 yr
Joshua: Confess (blame Jake)	1 yrs, 10yrs	5 yrs, 5yrs

Note, the only circumstance which would improve Joshua's and Jake's situation is a binding agreement to co-operate (deny) beforehand.

If the two men were not able to make a binding cooperation pact to remain silent before being arrested, they are engaged at the police station in what is known as a non-cooperative game.²⁴⁴ This type of game (a zero-sum, non-cooperative game)²⁴⁵ and game

²⁴⁴ "A cooperative game is a game in which the players can make binding commitments, as opposed to a non-cooperative game, in which they cannot." RASMUSEN, *supra* note 11, at 21.

²⁴⁵ DAVIS, *supra* note 12, at 38 (noting that in game theory, specifically in finite two person zero sum games, the minimax theorem operates). "The minimax theorem states that one can assign to every finite, two person, zero-sum game a value V: the average amount that player I can expect to win from player II if both players act sensibly." *Id.* This theorem allows the analyst to simplify the study of games by predicting a sensible course of action. "[T]he outcome is intimately related to *both* players' behavior and each is at the mercy of the other's caprice." *Id.* at 39. The term 'zero-sum' (or equivalently, 'constant sum') means the players have diametrically opposed interests. The term comes

theory can help us analyze the activities and predict the conduct in an oligopolistic marketplace similar to the electronic voting machine market.

In an oligopoly, each firm faces a situation much like a game. Each firm must choose a strategy, taking into account the other organization's strategies and reactions to its decisions.²⁴⁶ In the current voting machine marketplace, there are two principal suppliers: Premier and ES&S (and a third smaller supplier, Sequoia), that supply the majority of the machines to the fifty states.²⁴⁷ Complaints concerning the lack of accuracy²⁴⁸ of electronic voting machines attributable to deficiencies within the proprietary software or failure of the vendor to provide properly functioning machines are publicly reported.²⁴⁹ Yet the vendors,

from parlor games like poker where there is a fixed amount of money around the table. If you want to win some money, others have to lose an equivalent amount. Two nations trading make up a non-zero-sum game since both may simultaneously gain. *Id.* at 14.

²⁴⁶ Sagi, *supra* note 14, at 277.

²⁴⁷ *See supra* note 1.

²⁴⁸ *See supra* note 38.

²⁴⁹ *See* Nikita Stewart, *District's Primary Results Certified*, WASH. POST, Sept. 26, 2008, at B01 (reporting a glitch in the primary election held in Washington, D.C. in September, 2008 that could have possibly been an error with the Sequoia Voting Systems equipment); sources cited *supra* note 236. With regards to the primary issues in Washington, D.C., the Election Officials and Sequoia Election Systems are not quite sure what happened. Nikita Stewart, *Lawyers Will Monitor Polls Nov. 4*, WASH. POST, Sept. 30, 2008, at B02. The District of Columbia maintains that the problem was a faulty memory cartridge. *Id.* Sequoia, however, vehemently denies this and attributes the glitch to human error. *Id.* After controversy in the 2006 election in Sarasota County Florida, the county commissioners unanimously voted to end their relationship with ES&S, and instead have chosen to use Diebold voting machines. Patrick Whittle, *Sarasota Switches Voting Machine; County Dumps its Old Company and Cuts a Deal With a New Maker*, SARASOTA HERALD-TRIBUNE, June 7, 2007, at BS1. As of August, 2008, touch-screen machines set up in half of Ohio's counties didn't work properly, and the Secretary of State, Jennifer Brunner, wanted Diebold to pay for it. Mark Niquette, *Missing Votes Spark Lawsuit; Brunner: Touch-screen Machines Defective, Company Should Pay*, COLUMBUS DISPATCH, Aug. 7, 2008, at 01A. Brunner planned to file a lawsuit to get the money back from the equipment and to seek punitive damages after an investigation showed that votes in at least 11 counties were "'dropped' in elections when memory cards were uploaded." *Id.* Premier filed a lawsuit against the state saying that it had satisfied its obligations under the contract. *Id.* Florida, however, is choosing a different type of voting machine from ES&S (one that actually calls for the voter to make a paper vote, and not solely electronic) instead of the one used at the election in 2006, but it is not specifically stating that the reason is due to previous machine malfunction. Kathy Gill, *States Abandoning Touchscreen Voting Equipment*, ABOUT.COM, Aug. 18, 2008,

claiming trade secret and copyright protection, refuse to release the software for independent testing prior to an election, or independent auditing after an election, or change or alter their software allowing open source software.²⁵⁰ As a Princeton University computer scientist who conducted testing on Diebold (Premier) AccuVote-TS voting machines for code attacks wrote, “Mitigating these threats will require changes to the voting machines’ hardware and software and the adoption of more rigorous election procedures.”²⁵¹ Strangely, in the face of mounting criticism,²⁵² the DRE vendors have not been driven to

<http://www.uspolitics.about.com/b/2008/08/18/states-abandoning-touchscreen-voting-equipment.htm>. Furthermore:

One way in which fraud could occur is through the use of ‘homebrew’ smartcards. When voters show up at telling site, they are given smart cards that they insert into the DRE and that allows them to receive a ballot. Computer scientists found that attackers could create their own homebrew smartcards

. . . This danger was highlighted by the Compuware Report, a 246 page report commissioned by the state of Ohio, that examined the DREs of the four major vendors: Diebold, ES&S, Hart and Sequoia. The report found that the four-digit PIN code for the smart card “is a factory default from Diebold [that] cannot be changed . . . [and] was guessed in less than two minutes of testing.” Voters who are able to program their own smartcards have the ability to vote multiple times on a machine by ignoring the voting terminal’s deactivation command.

Carrier, *supra* note 3, at 657–58.

²⁵⁰ As recently as October 4, 2008, a DRE vendor, Sequoia has appeared in court in litigation concerning the accuracy of its machines and opposed the release of an independent test conducted on its machines by Princeton computer scientist, Dr. Appel regarding the accuracy, and security of its machines. See Diane C. Walsh, *Jersey Disputes Report Faulting Voting Machines*, STAR LEDGER NEWS (Newark), Oct. 18, 2008, available at <http://www.nj.com/news/ledger/index.ssf?/base/news-14/122430339766090.xml&coll=1>. Dr Appel’s report found that Sequoia’s machines could “be easily hacked, while a professor from Carnegie Mellon University scoffed at the findings, according to two divergent reports released yesterday by the Superior Court Judge presiding over the case challenging the machines’ reliability.” *Id.*

²⁵¹ See ARIE J. FELDMAN, J. ALEX HALDERMAN & EDWARD W. FELTEN, *Security Analysis of the Diebold AccuVote-TS Voting Machine* 1 (Sept. 13, 2006), <http://citp.princeton.edu/pub/ts06full.pdf>.

²⁵² *Id.* at 1 (“Analysis of the machine . . . shows that it is vulnerable to extremely serious attacks. For example, an attacker who gets physical access to a machine or its removable memory card for as little as one minute could install malicious code; malicious code on a machine could steal votes undetectably, modifying all records, logs, and counters to be consistent with the fraudulent vote count it creates. An attacker could

change and upgrade like most sellers in a competitive market by the market demand for upgrade in quality improvement. Even stranger, they have not been challenged by the entry of many new upstart firms eager to gain a foothold in a lucrative voting machine market fueled by government cash. The odd situation is reminiscent of novelist Lewis Carroll's phrase, "Curiouser and Curiouser," in *Alice's Adventures in Wonderland*.²⁵³

By viewing an analogous situation in a game, we should be able to translate the insights gained into a quantitative model. Subsequently, a review of that quantitative model allows us to make inferences concerning the behavior of the players.²⁵⁴

Historically, economists reviewed an oligopoly in terms of game theory.²⁵⁵ Game theory, an analytical tool utilized to comprehend interactions between persons when each person's actions affect the others,²⁵⁶ should help us predict the actions of the players in the oligopolistic DRE market. Game theory helps to explain how oligopolists maintain their actions and conduct around pricing. With so few firms in the relevant market, the firms are able to make pricing decisions with reference to the reaction of

also create malicious code that spreads automatically and silently from machine to machine during normal election activities—a voting-machine virus.”)

²⁵³ Lewis Carroll, the author of *Alice's Adventures in Wonderland*, was actually Charles Lutwidge Dodson, a mathematics teacher at Christ Church, Oxford. See Martin Gardner, *The Annotated Alice* xxiii (2000) (“He [Lewis Carroll] had a great fondness for playing with mathematics, logics and words, for writing nonsense and for the company of attractive little girls.”). Gardner identifies a quote in *Alice's Adventures in Wonderland*, as an allusion to game theory, where Alice and the Duchess, a strange character, engage in a long conversation: “‘Of course it is’, said the Duchess, who seemed ready to agree to everything that Alice said: ‘There’s a large mustard-mine near here. And the moral of that is—‘the more there is of mine, the less there is of yours.’” *Id.* at 92. “Carroll seems to have invented this proverb. It describes what in modern game theory is called a two person zero sum game—a game in which the payoff to the winner exactly equals the losses of the loser.” *Id.* at 92 n.7. In a zero sum game what one player gains, another player must lose.

²⁵⁴ DAVIS, *supra* note 12, at xv; Piraino, *supra* note 25, at 18 (“Game theory explains how oligopolists can maintain supracompetitive prices without entering into express price-fixing agreements. In an oligopoly, where there are so few firms in the relevant market, it is easier for firms to make pricing decisions in ‘reference to the likely reaction of competitors.’” (citations omitted)).

²⁵⁵ Werden, *supra* note 13, at 720.

²⁵⁶ WALTER J. WESSELS, *ECONOMICS* 432 (Barron's Educ. Series 2006) (1987).

their rivals.²⁵⁷ As asserted by one legal scholar, the oligopolists recognize their interdependence and the fact that “its optimal price is a function of the price charged by its rivals.”²⁵⁸ More importantly each firm is “aware that its competitors are armed as it is with weapons of price reductions, aggressive advertising and product improvement.”²⁵⁹

First, a game is started by naming the rules. The elements of the game are: players, actions, payoffs and information.²⁶⁰ The objective of the game theorist is to describe a situation in terms of the rules of the games in order to explain what will happen in that situation.²⁶¹ The rules also have to specify the steps or actions the players can take in a situation. For our purposes, the actions could include: allowing or restricting access; lowering or raising prices; offering or refusing to offer better quality; and/or better service. The rules would include the pertinent information each player possesses concerning the market, i.e. the demand for the products. The rules would also have to provide for the amount of information each player possesses concerning the other players. Finally, the rules would have to allow for information to include the profits each player receives from the steps taken by all players and the optimal profit which determines the outcome of the game.²⁶²

Two types of games are relevant to our study of oligopolies: one shot games²⁶³ and repeated games.²⁶⁴ One shot games are

²⁵⁷ Piraino, *supra* note 25, at 19.

²⁵⁸ *Id.*

²⁵⁹ *Id.*

²⁶⁰ GIBBONS, *supra* note 242, at 3 (“The normal-form representation of a game specifies: (1) the players in the game, (2) the strategies available to each player, and (3) the payoff received by each player for each combination of strategies that could be chosen by the players.”).

²⁶¹ RASMUSEN, *supra* note 11, at 12.

²⁶² Werden, *supra* note 13, at 721.

²⁶³ Werden opines that one shot games like the Prisoner’s Dilemma:

[A]re a mainstay of modern economic thinking about competition even though they are criticized for abstracting from the real-world fact that competitors meet again and again. Economists nevertheless believe one-shot game oligopoly models provide useful, if imperfect predictions of the behavior of real world oligopolies, and these models have been found to explain . . . reasonably well the levels of prices and profits typically observed in real-world industries.

those which are played only once whereas repeated games are those where the same game is played many times.²⁶⁵ A game theorist observed:

In game settings, such as the prisoners' dilemma game, each player's goal is to find her payoff maximizing strategy, taking into account the rival's strategy. Such strategies constitute a stable solution if neither player has an incentive to change her strategy, given the rival's strategy. The stable solution is called 'Nash equilibrium' after John Nash who developed the concept.²⁶⁶

Returning to the game theory application of the Prisoner's Dilemma in looking at how oligopolies work, we can see that normally the DRE vendors would always have an incentive to provide access. Access to the software ultimately creates an opportunity for a larger market share and increased profits.

For example, suppose you have two players—Vendor 1 and Vendor 2—and each produces the same type of voting machines,

Id. at 759. In a single shot game each individual oligopolist wants to maximize its profit at the end of the period and is not concerned about future actions. *Id.*

²⁶⁴ *Id.* at 765 (“Repeated game oligopoly models are not understood to make contrary predictions. These models show that pricing coordination is possible under certain circumstances, but very few economists take the models so literally that they believe coordinated pricing occurs without communication of any form. A widely held view is that repeated game models correctly identify what outcomes are possible in oligopoly, but which outcomes actually are achieved is determined by forces outside the models, including agreements among competitors.”).

²⁶⁵ Willard K. Tom, *Application of Game Theory to Antitrust*, 5 GEO. MASON L. REV. 457, 459 (citing JOHN NASH, *Non-cooperative Games*, 54 Annals of Mathematics 286 (1951)).

²⁶⁶ Sagi, *supra* note 14, at 277 n.11 (describing the Nash equilibrium). A Nash equilibrium occurs when all the players are simultaneously choosing the best strategy as a reply to the strategy of all other players. See RASMUSEN, *supra* note 11, at 26 (“Nash equilibrium [is reached] if no player has incentive to deviate from his strategy given that the other players do not deviate.”); Werden, *supra* note 13, at 765 (“Repeated game oligopoly models are not understood to make contrary predictions. These models show that pricing coordination is possible under certain circumstances, but very few economists take the models so literally that they believe coordinated pricing occurs without communication of any form. A widely held view is that repeated game models correctly identify what outcomes are possible in oligopoly, but which outcomes actually are achieved is determined by forces outside the models, including agreements among competitors.”).

yet neither DRE vendor provides access to their software. Access to the software impacts their profitability. Restricting access keeps prices high and earns increased profits. If Vendor 1 releases access to his software, Vendor 1 will gain business since buyers will choose the machine that provides more access, transparency and potential accuracy. Vendor 2, on the other hand, by refusing access will lose business. If Vendor 2 releases access to the software, and Vendor 1 does not, Vendor 1 will lose business. If both release access to their software and fares drop (either because other entities reverse engineer or allow buyers to duplicate the product) they will both be worse off, if the sales do not increase significantly.

Like the two prisoners, Joshua and Jake, the best individual strategy for Vendor 1 and Vendor 2 is to provide access to their software. If they are involved in a non-cooperative scenario, the best strategy for each firm individually is to provide a machine with access to the software. No matter what the other vendor does, the individual optimal strategy, or Nash equilibrium for each is to provide access.²⁶⁷ The following matrix²⁶⁸ represents the pay-offs in the two vendor (V1, V2) situation where the decisions involve providing access to software or denying access.

		Vendor 1 Provides Access	Vendor 1 Denies Access
Vendor 2 Provides Access	Vendor 1 gets: Vendor 2 gets:	\$100 \$100	-\$20 \$120
Vendor 2 Denies Access	Vendor 1 gets: Vendor 2 gets:	\$120 -\$20	\$30 \$30

Should one move before the other, that firm would likely gain a larger market share. That advantage, however, might be short-lived if the second vendor moved to allow access and a price war

²⁶⁷ See WESSELS, *supra* note 256, at 433.

²⁶⁸ This matrix is based on a payoff matrix describing strategies utilized by two players who are Airline Companies in WESSELS, *supra* note 256, at 433.

ensued. If this were a one-shot game (no likelihood of repeat play), the vendor who first moves to provide access gets the best payoff initially. Assume both parties are denying access and receiving profits of \$30 dollars, the incentive for both parties would be to move towards access. Assume Vendor 1 and Vendor 2 start out in the lower right-hand corner where both deny access. If Vendor 2 moves towards providing access and if Vendor 1 continues to deny access, Vendor 2 gets a \$120 dollar payoff. Of course, Vendor 1 would then have an incentive to move to provide access and his payoff would become \$100 dollars. Vendor 2 now also receives \$100 dollars. The incentive is to provide access. No matter what the other vendor does, the dominant strategy is to provide access. A positive outcome for consumers might be a dip in prices that could remove entry barriers, allowing new competitors into the marketplace.

Here's how the conduct of two hypothetical firms in an oligopoly might play out in the Prisoner's Dilemma game using price as a variable. Assume that if "Premiere" charges \$3 per item it can earn \$1000 per day. Meanwhile, ES&S can also earn \$1000 per day at \$3 per item. If Premiere drops its price and charges \$2 per item, it can earn \$2000 per day, but only if ES&S continues to charge \$3 per item. If Premiere charges \$3, and ES&S drops its price to \$2 per item, Premiere will earn only \$500 per day, while ES&S earns \$2000 daily. However, if they both charge \$2 dollars, then both will earn \$800 dollars a day.

	PREMIERE \$3	PREMEIRE \$2
ES&S \$3	ES&S: \$1000 PER DAY PREMIERE: \$1000 PER DAY	ES&S: \$500 PER DAY PREMIERE: \$2000 PER DAY
ES&S \$2	ES&S: \$2000 PER DAY PREMIERE: \$500 PER DAY	ES&S: \$800 PER DAY PREMIERE: \$800 PER DAY

The best strategy for both Premiere and ES&S acting individually is to charge the lower price. At the lowest price of \$2, each firm has an improved outcome regardless of the other's

pricing. This is identical to the Prisoner's Dilemma: best not to cooperate (confess) which for the hypothetical firms means both lowering the price to \$2 per item. The optimal strategy is taking the same action (charging \$2) independent of what the other chooses.²⁶⁹ In an oligopoly (two or fewer), the players are strategically interacting. One firm's action has a significant impact on the other. This condition is called mutual interdependence.²⁷⁰ No matter what the other firm/player does, ES&S has an incentive to charge the lower price. The payoff of the lowest price is always better because Premiere can always change its position. The reverse holds true for ES&S.

Remarkably, by pursuing their individual selfish interests and not agreeing on the lowest price, both firms end up worse off. Ironically, this position may be the best one for the consuming public operating the voting machines.

On the other hand, if everyone cooperates, the best payday occurs, where both parties agree to charge the higher price as shown in the upper left hand corner. Both parties get a payoff of \$1,000 dollars, if they could agree to the higher price.²⁷¹ This game is known as a zero sum non-cooperative game,²⁷² where each party chooses the best of the worst: low prices. Premiere does the same analysis and chooses the worst: low prices. This results in a stable point, as both choices coincide. Each party's dominant strategy is to defect from the agreement. No matter what the other party does, the individual will be better off defecting from any agreement to cooperate. Thus the Nash equilibrium here will be for both parties to cheat on the game.²⁷³ The main thing we learn

²⁶⁹ See *id.* at 442–44.

²⁷⁰ See *id.* at 385.

²⁷¹ *Id.* at 442–44.

²⁷² DAVIS, *supra* note 12, at 14 (“The term ‘zero-sum’ (or equivalently, ‘constant sum’) means the players have diametrically opposed interests. The term comes from parlor games like poker where there is a fixed amount of money around the table. If you want to win some money, others have to lose an equivalent amount. Two nations trading make up a non-zero-sum game since both may simultaneously gain.”).

²⁷³ Alan Devlin, *A Proposed Solution To the Problem of Parallel Pricing In Oligopolistic Markets*, 59 STAN. L. REV. 1111, 1118 (2007).

from game theory in single period zero sum games is that any agreements are likely to be highly unstable.²⁷⁴

Let's return to Joshua and Jake, the hackers in the game. Suppose the two belonged to an international gang that engaged in heavy-handed enforcement powers. Assume that the two had a pre-arranged binding agreement not to confess. In fact, if anyone confessed, they would either be physically hurt or not be allowed to share in the proceeds the gang amassed over the years. In the face of such an agreement, with a potentially binding punishing effect, the dominant strategy for each individual would shift. The dominant strategy for each hacker would be to "deny" and obtain the higher pay-off.

Let's re-examine the vendors conduct above using the Prisoner's Dilemma²⁷⁵ employing the Nash equilibrium²⁷⁶ in a repeated game. Remember, the Nash equilibrium describes a situation where persons interacting with each other choose their best strategy given the strategies that all the other persons have chosen. The Prisoner's Dilemma game is known as a two person zero sum game, where the players have no common interests.²⁷⁷ In a completely cooperative game, the two players have nothing but common interests. For example, two barges approaching each other in a river will both want to avoid a collision; a performing artist and an audio engineer will both want the performance to sound good; an air traffic controller and a airplane pilot will both want a safe landing.²⁷⁸

In a two-person non-zero sum game, the players have both competitive and non-competitive or cooperative elements.²⁷⁹ The

²⁷⁴ *Id.*

²⁷⁵ *See supra* note 11.

²⁷⁶ *See supra* note 13.

²⁷⁷ RASMUSEN, *supra* note 11, at 25 ("A zero-sum game is a game in which the sum of the payoffs of all the players is zero whatever strategies they choose. A game which is not zero sum is nonzero-sum game or variable-sum.").

²⁷⁸ DAVIS, *supra* note 12, at 81.

²⁷⁹ RASMUSEN, *supra* note 11, at 22 ("The Prisoner's Dilemma is a noncooperative game, but it could be modelled as cooperative by allowing the two players not only to communicate, but to make binding commitments. Cooperate games often allow players to split the gains from cooperation by making side payments-transfers between themselves that change the prescribed payoffs.").

DRE vendor firms have both competitive interests and interests in common or cooperative interests.

In repeated games, where there is either an infinite number of games or there is a finite number of games but where the end period is undetermined, it is possible for firms to maintain their collusive agreement.²⁸⁰ In fact, the incentive to remain in a collusive agreement may be higher because the one period benefit of deviating from the agreement is outweighed by the future and diminished prices where all of the parties deviate from the agreement.²⁸¹ Calculating all of the factors involved, which include each competitors' pricing, the likelihood of detection and the threat of punishment, the Nash equilibrium may well occur at the collusive level in a repeated game.²⁸² Using game theory in a repeated non-zero game application, the implication that the players will collude to arrive at their best strategy begins to emerge.²⁸³

Assume the two vendors ("V1", "V2") now have to decide if they should spend money on research and development to produce voting machines with increased security encryptions, and available software protections against specific voter glitches and malfunctions. The rules of this game are easily identified. If only one vendor (V1) spends more, it will produce better machines and will earn larger profits. If both vendors (V1, V2) spend more money on R&D, then the software will become obsolete faster for each machine. The result will be less profit for both vendors.²⁸⁴ The following matrix²⁸⁵ depicts the payoffs:

²⁸⁰ Devlin, *supra* note 273, at 1119.

²⁸¹ *Id.*

²⁸² *Id.*

²⁸³ *See generally id.*

²⁸⁴ *See id.* at 1117.

²⁸⁵ *See id.* at 1118.

CHOICES	Vendor 2 (“V2”) Spends a Little	Vendor 2 (“V2”) Spends a Lot
Vendor 1 (“V1”) Spends a Little	V2 gets \$200 V1 gets \$200	V2 gets \$300 V1 gets \$50
Vendor 1 (“V1”) Spends a Lot	V2 gets \$50 V1 gets \$300	V2 gets \$100 V1 gets \$100

If both parties were able to collude and agree not to spend money on development and research, they would agree to ‘spend a little’ and earn more profits. If they both pursued the maximum strategy, they would both ‘spend a lot’ because this is the ‘best of the worst.’ If the game is played repeatedly (the decision making), i.e., as in the marketplace, then the players become cognizant of the other player’s strategy and would both spend a little and not spend a lot on research and development.²⁸⁶

In order to keep the prices at a high level, the vendors need either collusion (cooperation), or a repeated game where they can detect the other player’s strategy and work to their advantage. Even with collusion, the incentive is to cheat unless the players, like Joshua and Jake, have a binding agreement: a threat.²⁸⁷ Each firm can profit from cutting its price as long as the other firm does not.²⁸⁸

Like Joshua and Jake in the international gang, the two firms have an incentive to cheat. But if they can make a binding agreement to co-operate, even if in a repeating game, they can ensure that they keep their profits at a supra-competitive level.²⁸⁹

²⁸⁶ See *id.* at 1119.

²⁸⁷ DAVIS, *supra* note 12, at 101 (“A *threat* is a statement that you will act in a certain way under certain conditions. . . . The purpose of a threat is to change someone’s behavior: to make that person do something he or she would not do otherwise. . . . A threat is effective only to the extent that it is plausible.”).

²⁸⁸ See Devlin, *supra* note 273, at 1119–20.

²⁸⁹ See *id.* at 1120.

Decision making in oligopolies involves price competition, as well as non-price competition. Just as cheating can occur in price competition, it can also occur in non-price competition as we saw in the Vendor 1 and Vendor 2 game concerning research and development. Either vendor could choose not to comply with the agreement and move to another position. Forms of non-price competition include: access, advertising, better service and better quality.²⁹⁰

Before we analyze the DRE oligopoly of the two leading vendors for their conduct using non-price competition variables in access, software security and transparent standards, let's examine another game. This time we'll use a repeated game presented by a game theorist involving miniature powdered beignets.²⁹¹

		Donut Shop II's Price in ¢ per dozen				
		25	24	23	22	21
Donut Shop I's Price in ¢ per dozen	25	(25, 25)	(0, 40)	(0, 30)	(0, 20)	(0, 10)
	24	(40, 0)	(20, 20)	(0, 30)	(0, 20)	(0, 10)
	23	(30, 0)	(30, 0)	(15, 15)	(0, 20)	(0, 10)
	22	(20, 0)	(20, 0)	(20, 0)	(10, 10)	(0, 10)
	21	(10, 0)	(10, 0)	(10, 0)	(10, 0)	(5, 5)

Both owners of hypothetical Donut Shop I and Donut Shop II can purchase mini-donuts, called beignet dots from a bakery supplier at 20¢ per dozen. Together their market share in a large metropolitan area amounts to 1,000 dozen beignets per day. Both donut shops have sold their product for 25¢ per dozen. At this level they both make a profit (\$25) and divide the market evenly—controlling all of the market for beignets sold in their area.²⁹²

The matrix represents the payoffs for the donut players. The first number in each box represents Donut Shop I's profit in dollars; the second number in each box represents Donut Shop II's

²⁹⁰ See Sagi, *supra* note 14, at 300–01; see also Devlin, *supra* note 273, at 330–33 (discussing the effects of quality regulation, advertising, and improved transaction terms).

²⁹¹ See DAVIS, *supra* note 12, at 85.

²⁹² See *id.* at 84.

profit in dollars. Donut Shop I is thinking of reducing the price from 25¢ a dozen. The products are virtually identical. Customers easily switch from one brand to another if the price is reduced. The lower price attracts virtually all of the sales in the market. Prices are posted each morning on the stores' signs.²⁹³

Profits are entered in the matrix. Those profits correspond to the set of prices charged by each vendor. If Donut Shop I, reduces its prices from 25¢ to 24¢, it will capture the entire market and reaps \$40 dollar profits, but only if Donut Shop II continues to charge 25¢. If Donut Shop I reduces its price to 23¢ and Donut Shop II simply reduces its price to 24¢, Donut Shop I still captures the market and earns \$30 dollars worth of profit.²⁹⁴

In assessing the payoffs for this game, several items become clear. The vendor should never charge 25¢ if a price change is made by the other vendor. Why? Because 25¢ is dominated by 24¢. If a competitor charges 24¢, he will always do better than his rival who charges 25¢. Nor should a vendor charge less than 21¢. Any price less than 21¢ will not return a profit.²⁹⁵

Once price cutting begins, 25¢ is ruled out. A competitor can always do better than his rival by charging 24¢. In fact, once 24¢ is reached by a competitor, the other vendor can always do better at 23¢. Until one reaches 21¢, the other competitor can always move and charge less thereby making more profit.²⁹⁶

Surprisingly, from a starting point of 25¢ where the players received \$25 dollars in profits and divided the market evenly, logical reasoning pushed the players to the 21¢ block where they earned \$5 apiece.²⁹⁷

Playing this game in a non-cooperative strategy results in the players reaching the lower price of 21¢ and reduced market profits of \$5. The game gets interesting if the players play it more than one time. If a player drops her price one day, the other competitor is sure to drop his price the next day; however, if the players

²⁹³ See *id.* at 84–85.

²⁹⁴ See *id.* at 85.

²⁹⁵ See *id.*

²⁹⁶ See *id.* at 85–86.

²⁹⁷ See *id.* at 86.

engage in playing over the course of several days, the incentive to drop prices changes. The players have an opportunity to observe the competitor's strategy. In addition, they can see where cooperation may bring greater payoffs than competition.²⁹⁸

The contribution of modern game theory is to show that the story becomes much more complicated if one studies a "repeated game," in which firms interact with the same rivals again and again, and know that they will do so. In such a setting, a firm must trade off the short-run gains from cheating against the future cost—in one version, the cost of never again receiving the supra-competitive price. In infinitely repeated games, in which the interaction goes on forever, or in games in which the end point is uncertain, the firms will be able to maintain the supracompetitive price if they are able to detect and respond to one "cheating" rapidly.²⁹⁹

Now, let's return to our examination of the DRE vendors. The vendors currently restrict access to the software for independent auditing and testing,³⁰⁰ experience repeated malfunctions with the machines during voting³⁰¹ and have been criticized for ineffective security and accuracy features.³⁰² They also claim copyright and

²⁹⁸ See *id.*

²⁹⁹ Tom, *supra* note 265, at 459.

³⁰⁰ See *supra* note 30.

³⁰¹ See Philips, *supra* note 7, at 1147 (noting Congress's Government Accountability Office was prompted to launch an investigation of the electronic voting machines by the number of problems in the 2004 election); Tokaji, *supra* note 2, at 1740 (noting that during the 2004 presidential election, one electronic voting machine in Carteret County, N.C., failed to record 4500 votes); John Schwartz, *Mostly Good Reviews for Electronic Voting*, N.Y. TIMES, Nov. 12, 2004, at A20, available at <http://www.nytimes.com/2004/11/12/politics/12evote.html> (reporting that some voters had to have their DREs restarted so that their true votes could be recorded). Tokaji notes that another electronic voting machine in Franklin County, Ohio, reported almost 4000 extra votes for George W. Bush; however, this error was promptly detected and corrected by election officials. *Id.* See generally HARRIS, *supra* note 7; RUBIN, *supra* note 7.

³⁰² See *supra* note 8; see also FELDMAN, HALDERMAN, & FELTEN, *supra* note 251, at 4 ("One style of [denial of service] attack would make voting machines unavailable on election day. For example, malicious code could be programmed to make the machine crash or malfunction at a pre-programmed time.").

trade secret protections for their software in denying access.³⁰³ Yet scientists have asserted that technology exists at a reasonable cost to build a DRE voting system—“including hardware, software, and election procedures”—that is secure and reliable.³⁰⁴

These decisions to deny access by the vendors are puzzling in light of the public outcry and demand for improved voting machines. Using game theory tools, it becomes increasingly apparent that the DRE vendors are acting cooperatively to further their own self-interests.

First, let's examine the options available to the vendors in deciding how to bundle their voting machine software with services. They could offer a machine which could include software only (“S”), or software with licensed access to the proprietary code (“SSA”) for random independent audits, or software with stricter encryption measures (“SSSE”), or software with the newest technology for security measures (“SSST”), or software licensed as open source (“SSSSO”) with all of the above available security measures. The vendors could also offer software with any combination of the above services. The profits received would be a function of the type of service offered: P{S}(software only), P{SSA}(software with access to the proprietary code for independent audits and testing), P{SSSE}(software with access and stricter encryption measures), P{SSST}(software with cutting edge technology for security and elimination of glitches) and P{SSSSO}(open source software with the above added improvements).

Initially any software with a new service would attract customers. Based on consumer preferences, the vendor (Vendor I)

³⁰³ Scholars Long and Massey have chronicled in detail the DRE vendors' arguments for copyright proprietary protection in their software. *See* Long, *supra* note 29, at 548–49; Massey, *supra* note 28, at 235. Critic Levine articulates the trade secret protections afforded software in DREs. *See generally* Levine, *supra* note 7, *passim*.

³⁰⁴ FELDMAN, HALDERMAN, & FELTEN, *supra* note 251, at 3 (“Despite these problems, we believe that it is possible, at reasonable cost, to build a DRE-based voting *system*—including hardware, software and election procedures—that is suitably secure and reliable. Such a system would require not only a voting machine designed with more care and attention to security, but also an array of safeguards, including a well-designed voter-verifiable paper audit trail system, random audits and forensic analyses, and truly independent security review.”)

offering the newer software package, will receive a larger share of the market. Its revenue will rise and its customer base will expand. It will gain customers, while simultaneously Vendor II will lose customers and revenue. In the interim, prices may begin to modestly decline as other firms enter the market, software open source licenses become competitive, and buyers seek other computer software developers to customize product. Vendor II will lose customers and revenue. Vendor II acting strategically may offer the new software at reduced prices or change the product offered. Ultimately the price will drop. Let's examine the best strategy for these two players.

In the beginning both vendors offer S (software only); they share the market equally and earn profits of X. What happens if one vendor defects and tries to offer the voting machine software machines with additional services and better quality? The matrix below displays the payoffs.³⁰⁵

		Vendor I's Choices ³⁰⁶				
		S	SSA	SSE	SSST	SSSO
2. Vendor II's Choices	S	50, 50	0, 80	0, 60	0, 40	0, 20
	SSA	80, 0	40, 40	0, 60	0, 40	0, 20
	SSSE	60, 0	60, 0	30, 30	0, 40	0, 20
	SSST	40, 0	40, 0	40, 0	20, 20	0, 20
	SSSSO	20, 0	20, 0	20, 0	20, 0	10, 10

Even in the face of an agreement, the best position of the individual vendor is to offer one or more of the new improved services if it wishes to gain customers, increase its market share and improve its profits. Any such move would cause its rival to rethink its position. There is no advantage for the firm in staying in the software only (no access) position when its rival firm moves to another position. In following the equilibrium strategies (and

³⁰⁵ See DAVIS, *supra* note 12, at 85.

³⁰⁶ Note: there could be any combination of the services offered by the vendors. It is in the best interests of the individual DRE vendor to defect and offer one or more of the bundled services. The vendor will always be better off offering one of the services.

there may be more than one) a firm's most dominant strategy is to offer improved services and quality to gain increased profits and market share.

In an oligopoly, we often see that the individual firms which normally would seek to maximize profits by pursuing individual competitive strategies act collectively to keep prices high, and maintain control of output.³⁰⁷ In an oligopoly, this collective action can occur if the players can make binding agreements to cooperate, like Joshua and Jake. The binding agreements can occur through overt action or tacit collusion.³⁰⁸

The matrix represents the profits of the vendors. The first number represents Vendor II, the second number represents Vendor I. Those profits correspond to the set of services offered by each vendor. If Vendor II provides a machine with access to software (SSA), he moves from a block (S) with 50% of the profit, to one with 80% of the profit because of increased market share and customer preference. This DRE (Vendor II) would capture the majority of the market. Vendor I's share would immediately drop to 0. If DRE Vendor II offers bundling to include increased encryption standards (SSSE), his share may drop to 60% profit but Vendor I's profit remains at 0 as long as Vendor I refuses to offer access. Now look at the positions if Vendor II moves to offer access to software (SSA) and subsequently Vendor I moves to offer access (SSA) immediately in a repeated play. They both reach market profits of 40%.

However, as soon as Vendor II moves to offer another improved product (SSSE), Vendor I's profit drops to 0 and Vendor II increases his share to 60%. Ultimately, one of the equilibrium points for both parties would be to offer SSSE (Software with access and increased encryption standards). At that point, neither

³⁰⁷ Shelanski, *supra* note 18, at 86.

³⁰⁸ Piraino, *supra* note 25, at 16 ("In a perfectly competitive market, with many competing firms and easy terms of entry and exit, firms must price at the market level (i.e. at marginal cost) or risk losing sales to competitors. However, in an oligopoly, where there are only a few sellers, it is easier for those sellers to cooperate to raise prices above the normal competitive level. Coordination among oligopolists can allow sellers to price above marginal cost at 'supracompetitive' prices." (citation omitted)).

party would have an increased incentive to move. Both parties would share market share of 30%.

Yet, an incentive to deviate and keep moving could occur. It would never pay to offer more bundling services than the open source (SSSSO) because the parties would barely earn a profit. In fact, the far right corner (10, 10) may represent the lowest profit return for the parties providing a complete set of services. However, the incentive to offer a machine with improved services exists as a Nash equilibrium point. The only effective way to maintain the highest prices (50, 50), in such a repeated game is to agree to maintain the pricing as it currently exists and refuse to offer improved services.³⁰⁹

In a one-shot game, like the Prisoner's Dilemma, the players have no opportunity to make promises about the future. Their Nash equilibrium is to not cooperate. Also, if they know their actions are interdependent, and yet they will never meet again for the next game, there is no incentive to react differently (i.e. to cooperate).³¹⁰ However, the outcome of the game changes if the vendors believe that there is a high probability that they will play the Prisoner's Dilemma repeatedly. In the face of a repeated game, rational cooperation between the two vendors becomes much more likely.³¹¹

As one theorist states, where the players always believe that there is a high probability that they will play the Prisoner's Dilemma again, and if this probability is large enough, with a sufficiently high payoff, the repeated game has many Nash equilibria.³¹² In some of these strategies, cooperation is always played on the equilibrium path.³¹³

³⁰⁹ See KEN BINMORE, *GAME THEORY: A VERY SHORT INTRODUCTION* 72–73 (Oxford University Press, Oxford, UK) (2007); Sagi, *supra* note 14, at 277 n.11 (“[E]ach player's goal is to find her payoff maximizing strategy, taking into account the rival's strategy. To solve the game, the game theorist needs to find the strategies that solve each player's problem. Such strategies constitute a stable solution if neither player has an incentive to change her strategy, given the rival's strategy.”); *infra* notes 310–13 and accompanying text.

³¹⁰ BINMORE, *supra* note 309, at 72.

³¹¹ *Id.*

³¹² *Id.*

³¹³ *Id.*

The DRE vendors control the product supply and the level of services for each type of machine. They operate in all 50 states and repeatedly conduct their activities.

By controlling output collectively and refusing to provide access, the firms in an oligopoly act like a monopoly. They sell the voting machines with a level of service and technological capacity at an inefficient level given the market demand for access to the software and accuracy in the output. Their output is produced less efficiently and at a higher cost to society than the output which could be produced by firms in a competitive industry. They fail to produce at a socially optimal output level.³¹⁴

This conduct and behavior is against the firms' self-interest and contradicts a social economic policy of a competitive marketplace offering maximum quality at an equilibrium price.³¹⁵ The oligopoly firms operate as a monopoly creating an inefficient market where the price of using the voting machines is artificially high and the quality of the product (numerous voting machine malfunctions) deliberately low.³¹⁶ Consider the conduct of a well known monopolist, Microsoft.

Microsoft, for example, has refused to disclose information on the interfaces to its Windows operating system, which are necessary for competing programmers to create applications that are compatible with Windows. It has been argued that Microsoft maintained the secrecy of such information to give its applications programmers a head start over those developing competing applications, as well as to preclude competing applications from evolving into an operating platform that ultimately could challenge the

³¹⁴ Piraino, *supra* note 25, at 16 (“Economists believe that such prices have two significant adverse effects. First, they harm consumers by transferring wealth from purchasers to producers. Second, they may cause purchasers to forego buying a product entirely.” (citations omitted)).

³¹⁵ *Id.* (noting that the potential losses from purchasers foregoing buying a product are “not offset by any gain to sellers”).

³¹⁶ *See id.* at 36 (arguing that protecting Microsoft’s monopoly “reduces Microsoft’s incentive to limit price increases and to continue to innovate in operating system products and services”).

dominance of the Windows operating system. In declining to disclose such information to outside programmers, Microsoft was acting against its legitimate self-interest. It would be in Microsoft's best interest to maximize the number of applications that utilize its operating system. Such a strategy would make Windows even more useful to consumers and maximize Microsoft's immediate revenue.³¹⁷

As in the case of the monopolist, there is no incentive for the two (or three firms) to improve quality by allowing access for pre-election logic and accuracy testing, or independent post-election auditing, or licensing open source software. Like the author asserts about Microsoft, when a monopoly [or oligopoly] acts against "its self-interest and makes it more difficult for competing applications to run on its system, it is reasonable to conclude that Microsoft's [or the oligopolists'] real purpose was to perpetuate its operating system monopoly."³¹⁸

Allowing access could reduce the price, lower the entry barrier and potentially entice other firms to enter and ultimately eliminate the exorbitant monopoly supra-competitive profits.³¹⁹

In the DRE marketplace, the preclusion of access for independent testing and auditing, the lack of improved security measures and the repeated glitches affecting accuracy, directly impacts a public good—the voting process. Using the game theory analysis, it is apparent that the firms should strategically provide access, or allow open source licensing or some variation which would maximize their individual profits.³²⁰

³¹⁷ *Id.*

³¹⁸ *Id.*

³¹⁹ *Id.* at 37 ("Like monopolists, oligopolists have a greater ability and incentive to engage in anticompetitive conduct than firms in less concentrated markets."). Piraino contends that courts should recognize that when oligopolists act collectively to maintain prices, they are exercising the same type of market powers as a monopolist. *Id.* He argues that such conduct harms consumers by "denying them the choice of alternative applications." *Id.* at 36.

³²⁰ See BINMORE, *supra* note 309, at 72–73.

Using a game theory analysis, the refusal of each of the DRE vendors to provide access or improved quality can only be explained by the existence of some type of cooperative conduct.³²¹ There are no governmental regulatory impediments to access. HAVA, which helped to fuel the oligopoly, does not prohibit access. There are no technological barriers since computer scientists have been analyzing these types of software problems for decades.³²²

A birds-eye view of one state's voting process highlights the control exercised by two oligopolists. Florida was the site of the 2000 election dispute that sparked the *Bush v. Gore*³²³ ruling. *Bush v. Gore*, in turn, was the impetus for the HAVA Act, which provided the cash that has resulted in the current DRE vendor oligopoly.³²⁴ In the November 2008 general election, sixty-seven of Florida's counties were to use machines that were the product of two or three vendors.³²⁵ The voting systems were the products of Premier Elections, ES&S and Sequoia.³²⁶

Florida's voting process has changed since the disputed presidential election of 2000. Like the majority of states, Florida now operates with DREs.³²⁷ These machines, while improving the

³²¹ HAVA does not require the vendors to restrict access to their proprietary software. See HAVA, Pub. L. No. 107-252, 116 Stat. 1666 (codified at 42 U.S.C. §§ 15301-545 (2006)); see also Piraino, *supra* note 25, at 18 (“[John] Nash emphasized that ‘interdependence is the distinguishing feature of games of strategy’ in that ‘[t]he outcome of a game for one player depends on what all the other players choose to do and vice versa.’ . . . In certain cases, players will choose to cooperate rather than to compete, because they will conclude that they have more to gain from committing themselves to a collective strategy with their rivals.” (citations omitted)).

³²² See generally Philips, *supra* note 7.

³²³ *Bush v. Gore*, 531 U.S. 98 (2000).

³²⁴ See 148 CONG. REC. H2597 (daily ed. May 16, 2002) (statement of Rep. Foley) (“[W]hether an Al Gore supporter or a George Bush supporter, no one's vote should have been called into question. . . . This bill brings us light-years forward in hoping to never revisit that time and that place again.”).

³²⁵ See Voting System in Use for the November 4, 2008 General Election, http://doe.dos.state.fl.us/voting-systems/pdf/VS_Web_Display_10-9-08.pdf.

³²⁶ *Id.* Premier Elections Solutions, Inc. was formerly Diebold Elections Systems. See Florida Division of Elections, Vendors of Certified Voting Systems, <https://doe.dos.state.fl.us/voting-systems/certified-vendors.shtml> (last visited Mar. 18, 2009).

³²⁷ Voting System in Use for the November 4, 2008 General Election, http://doe.dos.state.fl.us/voting-systems/pdf/VS_Web_Display_10-9-08.pdf. Thirty-one states

election administration process, are the products of private firms, fueled by federal dollars operating in an oligopolistic marketplace.

The voting process in Florida, like other states, precludes public access to the software for independent testing or auditing. In addition, local and state governmental entities rely on the vendors for training and support. Most of the counties listed do not provide the voters with paper ballots.³²⁸ However, many states have moved to a voter verified paper receipt.³²⁹ The public is left to vote on machines where glitches, vote tallying inaccuracies and malfunctions are possible.

No voting system, electronic or otherwise, can be perfect. The problem remains that if a dispute occurs involving the fundamental voting interests, the voting rights are subsumed within the intellectual property rights asserted by the DRE owners. Because the owners operate within an oligopoly, their collective financial interests are set to preclude the public from access to the inner workings of the machines to further their financial gains.

Two constitutional interests, voting and intellectual property rights, collide within these electronic voting machines. The alarming result of the vendor oligopoly is private control of a fundamental liberty interest.

operate with DREs. *See* Election Equipment 2008, VerifiedvotingFoundation.org, <http://www.verifiedvoting.org/verifier/> (last visited Mar. 18, 2009).

³²⁸ Voting System in Use for the November 4, 2008 General Election, http://doe.dos.state.fl.us/voting-systems/pdf/VS_Web_Display_10-9-08.pdf. Of the sixty-seven Florida counties, thirty-nine used DREs which could not provide a paper ballot on demand. *Id.*

³²⁹ *See* Election Equipment 2008, VerifiedvotingFoundation.org, <http://www.verifiedvoting.org/verifier/> (last visited Mar. 18, 2009). Of the states exclusively employing DREs in elections, Nevada and Utah were the only two states using DREs with voter verified paper receipts, while Delaware, Georgia, Louisiana, Maryland, New Jersey, and South Carolina used DREs that did not provide voter verified paper receipts. *Id.* Of the states that offered both paper ballots and DREs in elections, twelve states only used DREs with voter verified paper receipts, seven states, along with the District of Columbia, only used DREs without voter verified paper receipts, and four states used a mixture of DREs that provide voter verified paper receipts and DREs that did not provide voter verified paper receipts. *Id.* Nineteen states, along with Puerto Rico, did not use DREs at all. *Id.*

CONCLUSION

An oligopoly currently operates in the DRE voting machine marketplace where federal elections are conducted. A few vendors, fueled by federal dollars provided through the HAVA Act, supply the majority of the electronic voting machines to the fifty states. These few vendors refuse to improve the quality of their voting machines, provide access to the software or upgrade the technology of the machines to eliminate the numerous reported glitches, errors and malfunctions of the voting machines. These DRE vendors maintain that the federal and state intellectual property protections for their software, both copyright and trade secrets, protect their property interests in the voting machines and preclude independent access by the interested public for auditing, licensing and upgrading purposes. The fundamental liberty interests in voting and access to a fair and fraud-free election held by Americans is slowly being subsumed by the claims of intellectual property protections for the software.

Utilizing game theory, it is apparent that the firms in this marketplace collectively act to maintain prices, output and quality based on financial interests. Their pricing and output strategy is a function of the interdependence and pricing strategies of their rival DRE vendors. The individual self-interests of the vendor would dictate changes in the pricing and output decisions to allow access to the proprietary software of the DRE machines. Analysis of the DRE vendors conduct, using game theory, leads to the inevitable conclusion that these vendors are collectively acting against their individual self-interests in improving to maintain monopolistic control. The consequence of the oligopolistic market control is that the federal election process is held hostage to vendors' financial self-interest.

Given the importance of fair and fraud-free elections, the best course for resolving the conflict between voting rights and intellectual property rights would be for Congress to intervene. A redefinition of the HAVA Act, requiring DRE vendors to provide independent auditing and security testing, verified voter paper trials, increased security protections and certifications, and effective oversight from the EAC could protect America's most fundamental liberty. Whereas this would likely reduce the profits

2009]

INDIVIDUAL LIBERTIES AND IP PROTECTION

765

of DRE vendors due to an increase in competition, the American public would benefit.

Lacking Congressional intervention, the Courts will be required to resolve numerous anticipated voting disputes involving the DREs. Their task—balancing a fundamental liberty interest against a property interest within the context of an oligopolistic marketplace—priceless.

APPENDIX 1: VOTING SYSTEMS: STATE-BY-STATE³³⁰

VENDORS	NO. OF STATES SUPPLIED	STATES
1. Advanced Voting Solutions	2	Miss., Va.
2. AutoMark Technical Systems	0	
3. Avante International Technology	0	
4. Dominion	0	
5. Election Systems & Software ("ES&S")	39	Ala., Ariz., Ark., Cal., Colo., Fla., Haw., Idaho, Ill., Ind., Iowa, Kan., Ky., Me., Mass., Mich., Minn., Miss., Mo., Mont., Neb., N.M., N.Y., N.C., N.D., Ohio, Okla., Or., Pa., R.I., S.C., S.D., Tenn., Tex., Va., Wash., W. Va., Wis., Wyo.
6. Hart InterCivic	12	Cal., Colo., Haw., Ill., Ky., Ohio, Or., Pa., Tenn., Tex., Va., Wash.
7. MicroVote General Corp.	3	Ind., Ky., Tenn.
8. Precise Voting	0	

³³⁰ SOURCE: The information in Appendix I was obtained through corresponding state websites and state responses to a FOIA request for information regarding electronic voting machines. The twelve voting system manufacturers listed in Appendix I have registered with the Election Assistance Commission (EAC) and meet the requirements of Chapter 2 of EAC's Testing and Certification Program Manual. See Registered Manufacturers, U.S. Election Assistance Commission, <http://www.eac.gov/voting%20systems/voting-system-certification/registered-manufacturers> (last visited Apr. 21, 2009). Note also that Danaher Corporation (Mfg.) supplies to Del., Ky., and Pa. and that Unilect supplies to Va.

2009]

INDIVIDUAL LIBERTIES AND IP PROTECTION

767

9. Premier Election Solutions	31	Ariz., Ark., Cal., Colo., Conn., Fla., Ga., Ill., Ind., Iowa, Kan., Ky., Me., Md., Mass., Mich., Minn., Miss., Mo., N.H., N.Y., Ohio, Pa., Tenn., Tex., Utah, Vt., Va., Wash., Wis., Wyo.
10. Sequoia Voting	18	Ariz., Cal., Colo., D.C., Fla., Idaho, Ill., La., Mich., Mo., Nev., N.J., N.Y., Or., Pa., Va., Wash., Wis.
11. Truvote International	0	
12. Unisyn Voting Solutions	0	