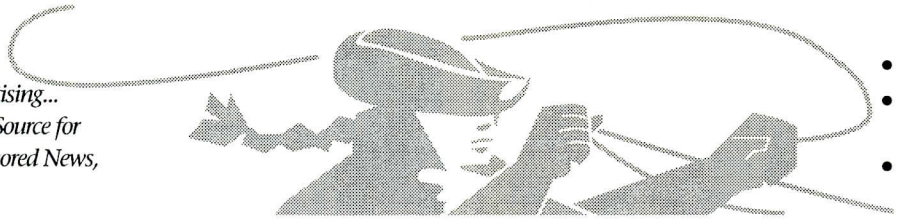
$7.95

Uncompromised by Advertising... Your Private Independent Source for Documented facts, Uncensored News, and Reasoned Analysis.



INSIDE:

- Secret Ballot, Secret Tally
- Modem Access to Your Vote
- Video Evidence of Vote Fraud?

RELEVANCE

This little black box is the PROM-Pak which carries the electronic instructions used in computer vote-counting. It could be counting the votes accurately and honestly or fixing the election. It all depends on what's inside . . .

PANDORA'S BLACK BOX

DID IT REALLY COUNT YOUR VOTE?

RELEVANCE · NOVEMBER 1996 · VOL. III · NO. V

[Editor's Note: When we began researching the integrity of the election process, we wanted to believe that the talk of "votescam" was just overblown hype. However, we have since discovered that the computer voting system in this country is a veritable can of worms, so open to tampering that if there is no organized election fraud going on, the criminals are falling down on the job].

SECRET BALLOT, SECRET TALLY

ELECTRONIC VOTING ON TRIAL

On November 5th, 1996, millions of Americans voted by secret ballot for thousands of elected officials from the Presidency to the local dog catcher. What few realized is that a key aspect of the vote-counting was also done in secret. What's more, they have been legally denied the right to find out precisely how their vote is counted.

How can this be? After all, everybody knows that each aspect of the vote-count is officially conducted by "the government" under the microscopic scrutiny of thousands of party officials, anxious candidates, poll workers, curious voters and the media, right? Not exactly. The counting of almost 70% of our votes is done inside a literal and figurative *black box* by a technical process that you have no legal right to inspect. The results from that black box are then counted by local election officials who send their results to the State where they are later "certified" as accurate and honest. But none of the certifying officials or the actual "vote-counters" at the board of canvassers or government officials at any other level has oversight of the thousands of votes counted inside these computers. Thus, they have no legitimate means of "certifying" that the results are accurate and honest. In fact, in numerous interviews, we found that no official at state, county, city or township levels has had any meaningful oversight (or even a clear understanding) of the vote-counting process at the crucial level of the election computers in each jurisdiction. Who does? A handful of computer vote-counting companies which have received surprisingly little publicity considering their central role in counting the vote. As a result, the public has near zero knowledge of these companies and the work they do.

SALTMAN... LISTED THE POSSIBLE METHODS BY WHICH "UNKNOWN PERSONS MAY PERPETRATE UNDISCOVERABLE FRAUDS"

Methods of vote-counting in the United States vary widely and include computer-counted punch cards (36%), computer-counted optically-scanned ballots (21.5%), direct-recording computer counters (4.3%) and mixed (some electronic, some mechanical) (8.3%). There are also the old-fashioned lever machines (approximately 27%), and the original method of hand-counted paper ballots (2.7%). [Note: figures were provided by the Federal Election Commission's Office of Election Administration and are based on a 1994 survey from the Election Data Service]. The computer-based systems were programmed a few weeks before the election by a surprisingly small group of vote-counting companies. Three major voting equipment vendors, Business Records Corporation (BRC) of Dallas, Texas; Sequoia Pacific of Jamestown, New York and Daneher Controls (whose system was formerly marketed by R.F. Shoup) of Gurnee, Illinois, and a handful of others, make products like the Optech Scanner and the Votomatic punch-card system which allow voters to either mark or punch holes in your ballot, which is then fed into a computer, where your vote is tabulated electronically. When the polls close, the voting tallies feed out from the back of the machine on a strip of paper that looks like a cash register receipt. These slips are then sent on to the County, the State and the media for further counting. In many heavily-populated areas, the Votomatic punch-cards or optical scan ballots are taken to a *central counting site* where they are fed into from 1 to 12 larger computers called tabulators at the rate of up to 1000 per minute.

ACCESS TO THE SOURCE CODES

What most people do not realize is that no one other than these obscure voting-machine vendors can examine the "source-codes" or computer-programming instructions that tell the computer exactly how to count your votes: not the voters, not the poll workers, not the city clerk, not the county election supervisor, not even the state elections director or any federal election officials are allowed to view the source-code. As impossible as it must seem, *Relevance* has verified this in dozens of interviews with state, local and federal election officials and state and federal computer voting consultants nationwide and even the vendors themselves. All admit it and none appeared the slightest bit concerned about it.

In order to understand the dangers of this system, we first have to go into the process of how computers count votes. Naturally, this is not an easy subject for those of us with little understanding of computers. Even people familiar with computer programming might think that the computer instructions for vote-counting would be rather simple (i.e. a brief "For/Next loop" would add a new vote each time a candidate is selected i.e.: "For x=x+1...Next") In practice, the vote-counting software is highly complex, because it not only includes the counter for each of dozens of candidates, which means they must prevent double-voting and allow people to vote straight ticket for all but one race, for instance, but it also includes ostensibly sophisticated security systems designed to keep out

would-be hackers. Ultimately, the programs reach into the tens of thousands of lines of code (eg. the program for the BRC Optech III-P Eagle scanner has 20,000 lines). In addition to making it harder for outsiders to tamper with the program, the size and complexity of these programs would make it easier for an insider (eg. one of the vendors' programmers) to conceal instructions or hiding places for instructions, which could later be inserted to rig a given race or even every race on the ballot.

Could the voting computers be pre-programmed to count votes in a way that favors a certain candidate — perhaps a candidate who has bribed a crooked company official or programmer? State election officials in Michigan assured us that this cannot happen because the computers are tested a day or two before the election in what is known as the "logic and accuracy test", which is open to the public. Generally, this amounts to a few dozen cards with various random votes being run through the machine to see if it counts them correctly. This is supposed to prove that the machine is honestly and accurately tallying the votes. But none of these officials even considered the possibility of hidden "subroutines" of programming code within the massive program which could suddenly interrupt the count and divert a few thousand votes from one candidate to another — a feat known as a "flip-flop" to experts concerned about potential computer vote fraud. Other potential dirty tricks which could be lurking inside Pandora's Black Box include the "Trojan Horse" (a set of commands concealed within the thousands of lines of code designed to rig the vote count and remain undetectable), and the "time bomb" in which the computer counts accurately until late in the tabulation when, after a certain number of votes have been counted, it suddenly begins to transfer every third or fourth vote meant for one candidate to his favored opponent.

Trapdoors and Trojan Horses

Howard Strauss, the director of Advanced Computer Applications at Princeton University, is a nationally-renowned expert in the field of computer voting. He categorically dismisses the efficacy of the so-called "logic and accuracy test" verification procedure. Strauss recently told *Relevance*:

> That turns out to be no test at all. That doesn't prove a thing. Any system that was designed with a 'trap door' or a 'Trojan horse' or any kind of fraudulent thing in it could pass that test easily...
>
> There are a hundred ways you could do this and probably any freshman in any school that teaches computer programming could figure out a half a dozen ways to do this. I've talked to folks who've said "oh no, we've fed a thousand votes in and then we looked at the other side and they were counted correctly." I said, "So what? That doesn't tell you what's inside the box."

Strauss explained further that since most computers have clocks and are programmed to be aware of the date, the machine could be set up so that the fraudulent counting activity only occurs on a given date, such as November 5th, 1996. *Relevance* raised this concern to Douglas Lewis, the director of the Election Center, a Houston-based project of the National Association of State Election Directors, an entity earmarked by the federal government to develop standards for election administration. Mr. Lewis dismissed the threat of such tampering, stating that the testing of the machines is done in many cases as late as 5 a.m. on the morning of the election and so would defeat a "time bomb" rigged to go off on that date. Similar statements were made by state and local election officials, betraying what skeptics of the system cite as their lack of understanding of the ease with which programmers could defeat the testing process — i.e., the same criminal who can instruct the computer to rig the count only on November 5th, can just as easily program this misbehavior to occur after the voting has already started — say at 11 a.m. or 3 p.m. The same computer clocks which keep track of the date are also aware of the time.

It seems the number of techniques for stealing the vote by computer is limited only by the ingenuity of the vote-rigging programmer. Howard Strauss added that computers can easily be programmed to count with perfect accuracy until a ballot with a certain particular set of candidate selections is fed through the machine. Since, on each ballot there are dozens of races, the number of possible permutations or combinations of votes on that single ballot is so large that a certain pre-set combination of votes could be used to trigger the computer to kick into "fraud mode". Strauss explains:

> You can tell the computer to behave badly in thousands of different ways. A common stunt used in other kinds of systems is to say to the computer, 'keep counting nicely until you see a vote for Perot, Nader, Clinton and Dole all on the same ballot.' So you say 'that'll never happen'.
>
> But what I do is I get a friend of mine to go into the polls early in the morning and vote this peculiar combination of people that I expect nobody is ever going to do because it's ridiculous and then what happens is, buried in the code, I have something that's looks for that strange combination...and then does it's bad thing... the program is waiting to see that.

Such a "votescam" would be best put to use at voter jurisdictions (Detroit and Cincinnati are examples) in which the punch card or optical scan ballots are taken from many precincts to a central counting site and fed into a few large tabulation computers which count ballots at the rate of up to 1000 per minute. The vote-counting is thus highly centralized and the central tabulators could be rigged to trigger major vote shifts when one of the above-described ballots appears.

The way it might work in practice is that a sophisticated programmer working within a computer vending firm could insert into the program a Trojan Horse, which would await the above-described combination on the ballot. Those seeking a certain outcome — say a vote to legalize casino gambling, or to support a taxpayer-

financed stadium for example — could be approached through intermediaries with a discrete offer to "guarantee" the election — for a price. The precise ballot selection needed to unleash the Trojan Horse would then be provided. Otherwise, the election would proceed honestly.

"A HOUSE WITHOUT DOORS"

Could such an illegal scheme work on a national scale? In a rare major media treatment of this taboo subject on election eve in 1988, CBS Evening News anchor Dan Rather asked Howard Strauss about the possibility of computer vote-rigging:

Rather: Realistically, could the fix be put on a national election?

Howard Strauss: Get me a job with the company that writes the software for this program. Then I'd have access to one third of the votes. Is that enough to fix a general election?

[Note: Strauss was referring to the software employed in the most commonly-used vote-counting computer program at that time. Incidentally, one company now has access to *over 50%* of the votes].

Strauss summed up the unverifiable nature of the system: "When it comes to computerized elections, there are no safeguards. It's not a door without locks, it's a house without doors."

That same year, the prestigious monthly, *The New Yorker*, carried a comprehensive, 32-page exposé of the dangers of computer voting, by Texas journalist Ronnie Dugger [See "Annals of Democracy — Counting Votes" in *The New Yorker*, November 7th, 1988 p. 40]. Dugger quoted Randall H. Erben, the assistant secretary of state in Texas, who served as special counsel on ballot integrity to President Reagan's campaign in 1984 and, in 1986, headed a similar group for the Governor of Texas: "I have no question that somebody who's smart enough with a computer could probably rig it to mistabulate. Whether that has happened yet I don't know. It's going to be virtually undetectable if it's done correctly, and that's what concerns me about it." Howard Strauss and Professor Eric K. Clemmons of the Wharton School of Economics have attempted to warn the public since the mid-eighties of the ease with which a skilled programmer could erase any evidence that he had tampered with the vote. Dugger summarized the findings of his numerous interviews: "All the computer experts I have spoken with agreed that no computer program can be made completely secure against fraud." He cited the opinion of Peter G. Neumann, of Stanford Research Institute, International in Menlo Park, California, who "emphasized the ease of concealing theft by computer 'without a trace'; characterized local elections as very vulnerable to fraud; and regards the theft of the Presidency by computers as entirely possible."

STAND UP AND BE MISCOUNTED

In 1988, Roy G. Saltman, now a retired computer consultant from the National Institute of Standards and Technology's Computer Systems Laboratory, wrote a landmark report for the U.S. Commerce Department entitled, "Accuracy, Integrity, and Security in Computerized Vote-Tallying", in which he exhaustively documented the many instances of vote mistabulation and the inherent vulnerability of U.S. voting systems to error and fraud. On page 23 he listed the possible methods by which "unknown persons may perpetrate undiscoverable frauds":

a) fraudulent alterations in the computer program or in control cards that manipulate the program

b) activation of a hidden program, possibly by means of a time-of-day match or with a specially encoded punch card ballot [Ed. Note: this is similar to the scenario that Howard Strauss had described]

c) manual replacement of the computer program by a fraudulent substitute

d) introduction of false ballots into the set of real ballots, through either addition or replacement; or introduction of false ballot data through interchange of ballots....

e) introduction of false voting summaries through changes in data stored in removable data storage units of precinct-located, vote-counting devices.

f) fraudulent alteration of the face of the voting device used by the voter at the polling location to mark a ballot or indicate choices.

g) fraudulent alteration of the logic of precinct-located vote-counting devices.

[Ed. Note: Mr. Saltman's publication is still available for $30.00 at James Condit's Precinct Project Institute Cincinnatus PAC, P.O. Box 11339, Cincinnati, OH 45211].

DOES ANYBODY CARE?

Critics say "where's the beef?" Have any of these computer programs ever been shown to malfunction? Saltman's 1988 report cited an extensive series of tests of the computer counting systems used in Illinois from 1983-87 which tested tens of thousands of ballots instead of the usual three or four dozen used in most pre-election tests. In the Illinois test series, it was discovered that significant errors in the computers' basic counting instructions were found in twenty percent of the tests. In 1988, Michael Harty, the Illinois director of voting systems and standards, pointed out that these gross "tabulation-program errors" would not have been caught by election authorities and lamented to *The New Yorker*, "At one point, we had tabulation errors in twenty-eight percent of the systems tested, and nobody cared."

Are these incidents cited by Saltman and many others inadvertent errors or deliberate "errors" — malicious fraud perpetrated by organized criminals paid by corrupt

power brokers? Most of the many instances of computer glitches and assorted snafus cited by Saltman were believed by election officials to be inadvertent. But, in our interviews with state, local and federal officials, the concept of computer-rigging of an election was politely dismissed as either impossible or at least so far outside the realm of likelihood as to be unworthy of serious discussion. Again, this was generally based on their unfounded faith in the hopelessly inadequate "logic and accuracy tests". Of course, these are the same tests which even some FEC consultants, like Robert J. Naegele — who tend to downplay the votescam threat — have admitted cannot detect Trojan Horses in the source-code unless, as in the Illinois series, tens of thousands of ballots are tested (and, if Strauss and others are correct, even these tests can be easily defeated).

COMPUTER RECOUNTS — "GARBAGE IN, GARBAGE OUT"

If there is rampant computer election fraud, we should have instances of discrepancies between the "official" computer-derived results and those of recounts in contested races. But this presumes the integrity of the recount and, unfortunately, most of them are done by simply feeding the punch-card or optical scan ballots right back into the same computer machines, which, if rigged properly, should produce identically phony results on the recount. As programmers like to say, "garbage in, garbage out". Hand recounts are the best way to detect telltale discrepancies between the computer results and the true vote. However this method is generally avoided since it greatly increases the time and staffing required. Also, if the loser in, say a city council race, demands and receives a hand recount, the many other races on each ballot will not be recounted, so a rigged senatorial, mayoral or other race would go undetected.

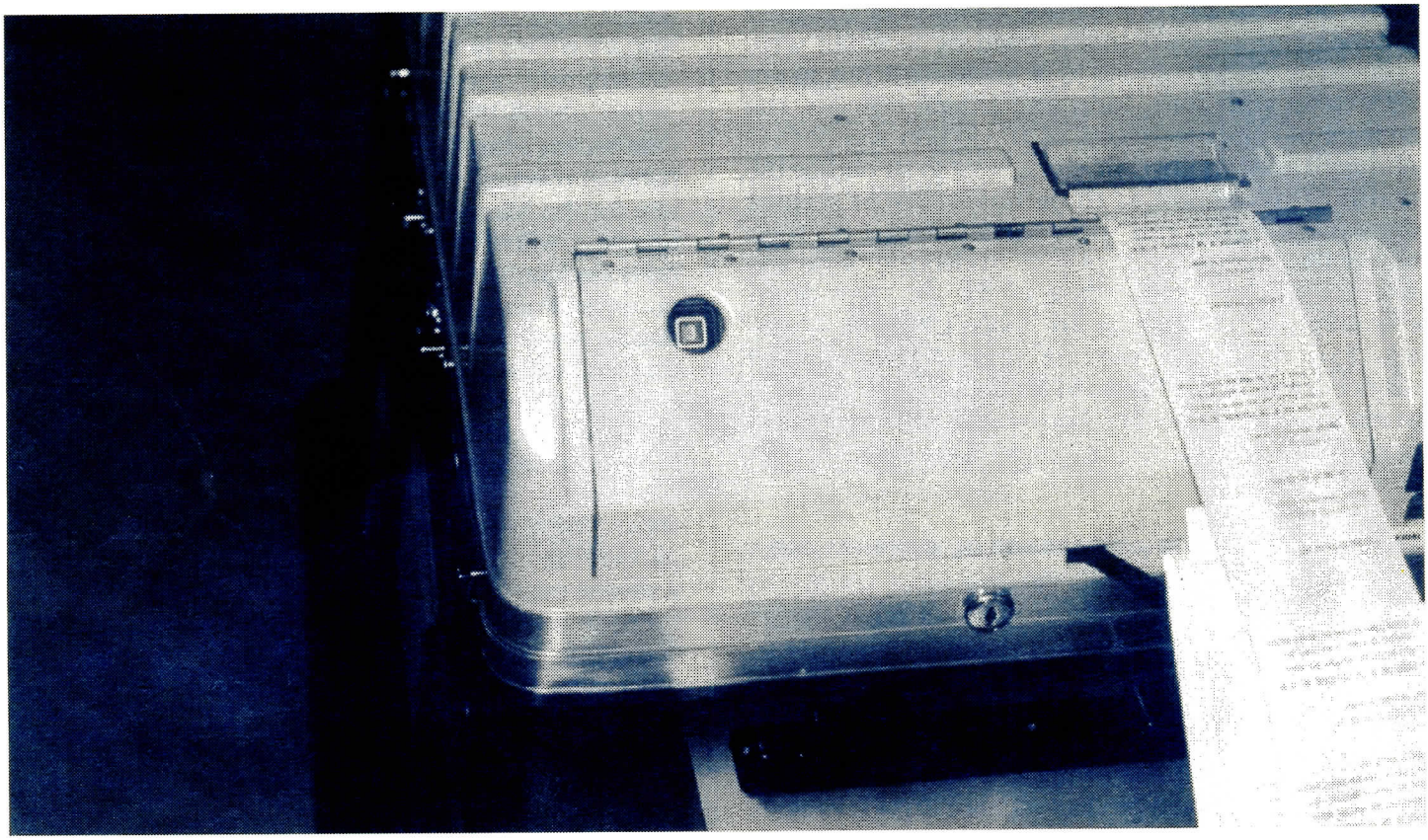
Nevertheless, Roy Saltman's report for the Commerce Department included dozens of often detailed presentations of cases in which computer errors were detected by suspicious candidates or alert election workers who obtained hand recounts. Generally, the mistabulations were attributed to human error. Willful misconduct was not often seriously considered. Still, several ended up in court, including some with criminal charges against vendors or election officials, as happened in one West Virginia case in 1981, in which the election supervisor, a candidate, a prosecutor, a county commissioner, election workers and the voting machine vendor were all sued by a group of candidates who believed that they had been cheated in the election. Mr. Saltman told *Relevance* that there is no way to know of all instances of vote-counting irregularities and his report was only a sampling. He explained that media coverage has not educated the public to the dangers: "when there is a problem locally it is almost never reported nationally, it's only reported locally." *Reader's Digest* offered an exception to this rule in June of 1995 with an article entitled, "Votefraud: A National Disgrace" . Although they focused primarily on illegal voters instead of illegal vote-*counting*, it served to show the number of people who are willing to participate in voting fraud.

SOMETHING'S ROTTEN IN MASSACHUSETTS

One recent example of a local story with little or no national coverage was the November Democrat Primary race for the Massachusetts' 10th District seat in the U.S. Congress, where challenger Philip Johnston — who had been declared the winner over entrenched Democrat nominee, William Delahunt — lost the nomination on a bizarre second recount. Johnston told *Relevance*: "the court looked at some disputed punchcard ballots which had already been declared to be blank and the court declared them to be actual votes." Suspiciously, 756 of the 968 disputed punchcard ballots came out of the same community — Weymouth, Mass — suggesting that either "Weymouthenians" are shamefully inferior card-punchers than their neighbors in the rest of the state, or someone may have tampered with the ballots. The State's Supreme Judicial Court examined the suspect ballots to determine "voter intent" by detecting "dimples" and other faint markings and somehow ended up awarding 469 votes to Delahunt and 177 to Johnston, thereby reversing the latter's victory. *The Boston Globe* of November 9th, 1996 wrote, "...there was no explanation why the high court ruled that the bulk of disputed, partially punctured punch-card ballots from the town of Weymouth should be counted in Delahunt's favor instead of as blanks." Johnston called the decision "unconscionable" and told *Relevance*: "We feel very strongly that they were wrong." What would he do to fight the apparent fraud? Johnston said, "I'm not sure what I can do now except help to make sure other people aren't victimized in the same way." With the help of "unfortunate mistabulations" like these, and despite the lack of national media focus on the problem, the gullibility of the American voter is wearing thin and a rising sense of distrust appears to be seeping into the mind of the voting public.

A RARE PEEP INSIDE PANDORA'S BOX

Apologists for the current voting system claim that there have never been any convictions for computer vote fraud and that it is "virtually impossible" to perpetrate. In the West Virginia case cited above, although the criminal charges were dropped, the judge had not allowed the jury to see a demonstration by the plaintiff's attorneys' computer expert, Wayne Nunn, Ph.D, a project scientist for Union Carbide, who had designed multimillion-dollar computer networks. After a nine-hour examination of the CES (now Business Records Corporation) computer system in question and in the presence of the CES president, the system's programmer, and others, "Nunn, with one punch card, added ten thousand votes to the total of one of the candidates in a mock race for President." [*The New Yorker*, November 7th, 1988, p. 68]. Nunn subsequently gave a deposition under cross-examination and revealed seven ways in which the system could be deliberately caused to miscount votes,



After the polls close, the machine produces a printout with the precinct's vote totals, which are then taken to the county for canvassing on their way to final certification by the state. Inside the back of this machine lies the PROM Pak which contains the computer's secret vote counting instructions.

including by manipulation of the toggle switch on the front of the machine to alter vote totals and by inserting a set of secret Trojan Horse commands into the source-code software as described earlier. So it can be done. But can it be detected and prosecuted?

A methodical expert analysis of the company's source-code could have been the key to determining the existence of fraud, but CES officials asked presiding Judge Charles H. Haden II, of the United States District Court, to block Nunn from inspecting their code on the basis that it was a "trade secret". Ultimately, the judge ordered that Nunn alone be allowed to view it, but without the computer he needed for a proper system analysis. Nevertheless, he discovered "trap doors", "wait loops", and "Christmas trees" which could all serve the same end of undetectable vote fraud. According to *The New Yorker*'s Ronnie Dugger, after viewing the code for several hours, "Nunn was prepared to testify that a 'debugger' in the BT-76 program, while enabling a programmer to make repairs in the program, was also a Trojan Horse; Haden excluded such testimony". Nunn was allowed to testify that "he had concluded that the program had been altered during the counting". The jury was also barred from seeing Nunn demonstrate how he could alter the vote count.

The case of Wayne Nunn being allowed to examine the proprietary source-code of the CES system is an extraordinary exception. The fact is that very few individuals outside of the computer vendors have ever been allowed to inspect the source-code of that or any other election equipment company. This was confirmed by Eva Waskell, the director of the Elections Project at Computer Professionals for Social Responsibility in a 1993 report entitled "Overview of Computers and Elections":

> Many court cases involving allegations of fraud were brought against vendors of electronic voting systems. There were no convictions. Was there ever any proof of tampering presented? No. Part of the reason for this may be that during the litigation *the plaintiffs were never given access to the vote tabulating program,* and hence there was no opportunity for anyone to establish evidence to either prove or disprove the allegations [Emphasis added].

We should point out that even if the court allowed the plaintiff's experts to inspect the source-code, there would be no proof that the code provided to the court was, in fact, the selfsame code used in the particular election in question. Federal election officials say that a few states are mandating that the source-code be placed in escrow so that it could be examined in the event of a particularly "fishy" election result. Florida, Michigan and California have such a system. This seemed to provide a hefty insurance against fraud — on the surface. But when we asked officials at the Michigan Board of Elections where they kept their escrowed source-code, we found that the state of Michigan doesn't have anything to do with the process. The code is transferred to an independent escrow agency by the computing machine vendors and *there is no state representative on hand to verify and sign off on the transfer.*

This was confirmed by Dan McGuiness of Business Records Corporation, which services many Michigan jurisdictions. In other words, there is no "chain of evidence" procedure for ensuring that the general purpose version of the software turned over to the escrow agents by the vendors wasn't switched before it was "initialized" and inserted into each computer sent to the individual elections. It should be noted that, when the software is placed into the precinct counting computers, it is converted into "machine language" and cannot be translated back into source-code for comparison with the copy in escrow. We have thus placed the integrity of a large part of our vote at the mercy of the moral standards of people we don't know — *and we don't even know that we've done it.*

ELECTIONS Я US

Several critics of the computer election fraud concept downplay the dangers by arguing that any programmer inside a large computer vendor who is bent on, let's say, rigging the election in favor of Bill Clinton, would run the risk of accidentally shooting himself in the foot, unless he knows the ballot position of the candidate (first, second..etc.). Since he has no control over some county clerk in Tupelo, Mississippi who might plug Bill Clinton into the top, middle or bottom of the ballot depending on how she feels that day, he will have an equal chance of shifting the illegal votes to Bob Dole or Ross Perot. However, this argument does not hold up when one considers that in many, if not most cases, the computer vendors either input the candidates' names to the ballot themselves or know the ballot positions in advance of their sending out the computers. According to Doretha Blair of the Michigan Board of Elections, the order in which political parties appear on the ballot is determined according to pre-set guidelines: "there's no happenstance on the ballot positions". She informed *Relevance* that whichever party currently occupies the office of Secretary of State appears first on the ballot. The other parties appear according to their pre-determined ballot status. The names of contenders in primary elections and the many non-partisan candidates, such as those vying for judgeships, are selected by alphabetical order and rotated according to precinct.

Who decides the order of precinct rotation in the judgeships and other non-party races? Doretha Blair told *Relevance* "As a rule, the counties will leave that rotation portion to the vendors". Thus, there is very little left up to chance for the hypothetical vote-fixing "mole" lurking within a vending company supplying the state of Michigan. If he knows the party of the Secretary of State and how to alphabetize, he can ensure that the computer illegally transfers votes to the right position on the ballot to favor his candidate. Although every state is different, its not likely that he'd have a much tougher time in Tupelo, Mississippi — or many other states for that matter. Such is the extent of the vote-counting machine vendors' stealthy takeover of the election process in much of the United States. To paraphrase Clemenceau, from the standpoint of the vendors, "elections are much too important to leave up to the election officials".

VOTE-RIGGING MADE SIMPLE

How would a sophisticated vote-fixer go about rigging an election? Ronnie Dugger interviewed one expert who explained how someone could fix the vote of any candidate. Computer scientist, Michael Shamos, Ph.D of Carnegie-Mellon University in Pittsburgh, had been a consultant for the Pennsylvania Bureau of Elections during the eighties. He was a major critic of the CES (now Business Records Corporation) Votomatic punch-card computer-counting system, which he described as "a security nightmare, open to tampering in a multitude of ways." Shamos viewed as a very real threat the same scenario presented by Howard Strauss: that a vote-fixer could walk into the polls and vote a specially prepared ballot, which, when it arrived at a central vote-counting site, would be fed into the computer and would proceed to "change the current vote total for any candidate desired."

Could a national election be fixed? As an illustration, Shamos laid out the following scenario for he and his hypothetical henchmen:

> Here's what we do. Working in a company headquarters, I'm writing some election software, which will be sent by Federal Express to jurisdictions in executable object code. I'm going to program this thing so that if there are more than eight hundred people voting in a precinct I'm simply going to trade some votes, take them from other parties and dump them into the party that I want to win. So all the totals are going to be exactly right.
>
> I'm going to change ten per cent of the votes, or five per cent — some small number — and that software is going out to pivotal jurisdictions in the country. And that is going to shift the national election.

Eva Waskell told *Relevance* that the most likely election-rigging scenario would entail picking key states, counties and precincts rather than going after the entire vote. This would ensure that the vote switching isn't too far out of line with public expectations. "What you would do to prevent that is to know how these precincts have voted in the past and just modify them a little bit. You pick the swing precinct in a heavily populated county and that's the one you fiddle with. Three to five per cent is enough to have the election outcome changed."

Indeed, the importance of heavily-populated "swing jurisdictions" was illustrated in the November presidential election, as seen in a report by *USA Today* of November 8th, 1996: "Bob Dole won more counties than Bill Clinton....1580 to 1534. But Clinton won more heavily populated counties in vote-rich states — and a second term." Dugger's article also quoted Peter Vogel, a consultant for the Texas Secretary of State, who agreed with Shamos that the Presidency could be stolen by computer "because of the electoral college...If you have a majority in the right states, it doesn't matter who has the majority of the votes in the country. If you program the right states for the right elections, I think you could control the Presidential results."

PAUSIBLE DENIABILITY

But what if a suspicious losing candidate insists he wants a hand recount and manages to prevail over the loud objections of election officials? Since the "index of suspicion" of major computer fraud is so low among election officials, it would be viewed as a computer error. Shamos told Dugger that if a computer program "didn't count correctly" (as happened in 28% in the state of Illinois test series noted above), it would likely be returned to the factory, where, according to Shamos, "the programmer would simply say there had been a glitch on the tape, or a bad ROM — a unit embodying read-only memory — or some other technical mumbo-jumbo". He suspected the same thing would happen if a recount of an actual election exposed deliberate "errors" in the program. Thus, "plausible deniability" is built into any discussion of computer errors between company experts and computer-illiterate election workers. But what about the honest employees of the company? Shamos doesn't see a problem for the vote-fixer:

> It's easy for a programmer. And his superiors will never find it. There's no way to find it unless they do an exhaustive code audit themselves. And this is a solo effort — one guy who happens to be well-placed. Of course, many others are involved, but they don't know [*The New Yorker*, November 7th, 1988].

The threat of manual recounts could be reduced if vote-fixers within a vendor had accomplices inside the election boards of their swing counties (accomplices whom they have perhaps "installed" by fixing their votes in return for their agreement to purchase the vendor's election equipment). In this scenario, if a hand recount simply cannot be avoided, the election officials will have a couple of weeks during which to alter the ballots. As Eva Waskell told *Relevance*, "So, let's go recount the punchcards. All this evidence is in the custody of the defendants who can block access to it for weeks after the fact. It is a system that is rigged against anyone trying to find proof." In addition, *Relevance* has learned that the larger vendors offer "one-stop" election supply shopping, which happens to include blank ballots of every type, the "locking mechanisms" (ballot box seals), "secrecy envelopes", ballot boxes, and transfer cases. One photo in the BRC sales literature promotes the seals used to lock the ballot boxes. Michael Shamos told *The New Yorker* that "blank punch-card ballots were easy to obtain; and the plastic seals on the boxes...were easily duplicated." If the computer machine vendor also sells the ballots and the seals, what's to stop a crooked employee from funneling duplicates to his "kept" election officials, in the unlikely event a hand recount is forced in a computer-rigged precinct?

THE ONLY THING WE HAVE TO FEAR...

Douglas Lewis, the director of the Election Center disagrees. When *Relevance* asked Mr. Lewis whether voters should be concerned by the warnings of experts like Shamos, Wayne Nunn, Strauss and others, he responded:

> When people fear the electronic systems, it is based on just that, fear...So far, all we've heard from those who try to raise phantoms and ghosts is the old argument from the Joseph McCarthy days of "there is a communist under every bed". But until somebody can show us that this sort of thing is happening, it's like being asked, "are you still beating your wife?"

Mr. Lewis used the word "fear" about nine times during our conversation. (e.g. "fear is fear. It's not based on logic"). When we asked about the general threat of computer election rigging, he responded "For you to be able to rig the software so that you could get by the logic and accuracy tests of all those jurisdictions, the odds would be 30 billion to one". We responded that people like Howard Strauss of Princeton and Peter Neumann of Stanford Research Institute believe logic and accuracy testing is a joke. He then stated "What I'm saying to you is that the odds are against it. Fear is such an ugly thing..." When he asked us why none of these experts were able to rig a vote-counting computer, we cited the fact that Wayne Nunn was able to change ten thousand votes on the C.E.S. computer by inserting a single punch-card. When we asked him whether he was concerned that nationally-renowned computer-voting experts from Princeton, Stanford Research Institute, the National Bureau of Standards and Xavier University had all raised grave concerns about the integrity of computer voting, Mr. Lewis responded "They are dealing from fear."

[Editor's Note: For the first time, we began to feel the icy finger of fear when we realized that those in charge of developing safe election standards had no fear of sophisticated computer vote fraud].

THE CINCINNATI ELECTION WIRETAPPING SCANDAL

Lewis and other skeptics of the vote-fixing scenario like to insist that there has never been any evidence of a "conspiracy" to fix elections by computer. But then, most of those we interviewed on both sides of the issue had never heard of the case of Leonard Gates of Cincinnati, Ohio. An employee of the Cincinnati Bell telephone company, Gates was watching a local t.v. news story, in which a Cincinnati man named Jim Condit, Jr. was charging that the election system was vulnerable to vote fraud in the Hamilton county election process. He based his charges on his experience as a candidate for city council in 1979, when, after an election night computer crash, Condit and seven other "feisty challengers" had suddenly "fallen to the very bottom of the heap" of 26 candidates. Gates called the station and later contacted Mr. Condit, telling him he knew firsthand how his votes were robbed. They met and shared information and ultimately Gates testified in Condit's Cincinnatus PAC (political action committee) lawsuit against the Hamilton County Board of Elections. The suit had earlier been decided against the plaintiffs and Gates took the stand during the appeal. He swore under oath that he was ordered by his Cincinnati Bell superiors to wiretap the election headquarters' phones lines to provide a link-up between the county's vote-counting computers and parties unknown (to Gates) on another phone line somewhere in California.

The following are excerpts from the *Cincinnati Post* of October 30th, 1987:

> Cincinnati Bell security supervisors ordered wire-taps installed on county computers before elections in the late 1970s and early 1980s that could have allowed vote totals to be altered, a former Bell employee says in a sworn court document.

Leonard Gates, a 23-year Cincinnati Bell employee until he was fired in 1986, claims in a deposition filed Thursday in Hamilton County Common Pleas Court to have installed the wire-taps. Cincinnati Bell officials denied Gates' allegations that are part of a six-year-old civil suit that contends the elections computer is subject to manipulation and fraud.

Gates claims a security supervisor for the telephone company told him in 1979 that the firm had obtained a computer program *through the FBI that gave it access to the county computer used to count votes.* [Emphasis added].

The FBI refused comment and Cincinnati Bell spokesmen vehemently denied the allegations, claiming Gates was a "disgruntled ex-employee", yet, 15 months later, on March 17, 1989, *The Cincinnati Post* ran a front page headline: "Police took Bell's truck for wiretap" — generated by four retired policemen who called a press conference to confirm Gates' allegation that a Cincinatti Bell truck was used in illegal wiretapping. Cincinnati Bell, immediately contacted by *The Post,* did not dispute that their truck was used, but claimed no knowledge of the illegal act. *The Post* of October 30th, 1987 continued:

In the deposition, Gates claims he first installed a wire-tap on a telephone line to the county computers before the 1977 election at the instruction of James West, a Bell security supervisor.

Gates contends both West and Peter Gabor, security director, told him to install wire-taps in subsequent elections. Both men declined comment Thursday.

In the 1979 election, which is the focus of the deposition, - Gates said he received instructions in the mail from West about installing wire-taps on county computers in the County Administration Building at Court and Main streets.

The wire-taps were installed on the eve of the election at Cincinnati Bell's switching control center at Seventh and Elm Streets and terminated in a conference room in the building, Gates alleges.

In the deposition, Gates described in great technical detail installation of the wire-taps.

At about 8:30 p.m. on election day - Nov. 6, 1979 - Gates said he was called by West and told something had gone wrong, causing the elections computer to malfunction. At West's instructions, Gates said he removed the taps.

The elections computer shut down for two hours on election evening due to what was believed to be a power failure, Condit Sr. has said.

Gates said West told him they "had the ability *to actually alter what was being done with the votes.*"

Gates said West told him the Board of Elections did not know about the taps and that the computer program for the elections computer "was obtained out of California, and that *the programming had been obtained through the FBI ...* "

Shortly after the 1979 election, Gates said he met with the late Richard Dugan, former Cincinnati Bell president, to express his concerns that the wire-taps were done without a court order.

"Mr. Dugan said it was a very gray area . . . This was just small compared to what was going on. He told me just, if I had a problem, to talk to him and everything would be okay, but everything was under control," Gates said [Emphasis added].

[Editor's Note: This scandal's alleged FBI connection raises the possibility of U.S. law enforcement and/or intelligence involvement in electronic vote rigging.]

Another Cincinnati Bell employee, named Bob Draise, admitted to being involved in a second phase of the illegal operation, which involved wiretapping several prominent Cincinnati political figures including a crusader against pornography named Keating and the Hamilton County commissioner, Allen Paul. Jim Condit told *Relevance* that "...faced with the testimony of *two* former Cincinnati Bell employees, a thinly transparent 'damage' control operation was launched." On March 4, 1989, the *Cincinnati Enquirer's* front page top headline read: "Ex-officers admit 12 illegal wiretaps. Although the five retired officers, one a former police chief, admitted only a small fraction of what the whistleblowers alleged, another wiretapping allegation was begrudgingly confirmed. The alleged involvement of the FBI was never pursued and the Bureau itself did not follow up on the Gates allegation. In spite of all the evidence, the appeal by the plaintiff failed and the issue was laid to rest.

BLIND FAITH

Before Gates and Draise's shocking charges surfaced during the appeals process, Condit's side had already gained one earthshaking concession from the court: Judge Richard Niehaus ruled "There is no adequate and proper safeguard against the computers being programmed to distort election results." This finding had followed an exhaustive hearing of testimony from experts on both sides of the issue. One of them, Robert C. Strunk, a veteran computer systems expert from Xavier University, testified for the plaintiff that after analyzing the entire Hamilton County election process, he determined that "it would require an act of faith for the members of the BOE to 'certify' that the vote count generated by this computerized system is a true and accurate count". Even local election officials reluctantly provided supporting testimony. *The Cincinnati Post* carried a report about the sworn courtroom testimony of Mr. Jim Bell, director of Cincinnati's Regional Computer Center, on November 30, 1989. "I was in the courtroom when Mr. Bell, under direct questioning, said that, if indeed a knowledgeable person had the source-codes, he would have a 100% chance of altering the election results, if he wished to do so," Condit told *Relevance.* Currently one of the most effective activists against vote-counting fraud in the country, Jim Condit recently wrote: "Despite Strunk's devastating expose of the weaknesses of the system, the Judge failed to provide a remedy to the wrong he had diagnosed, and the same [IBM punch-card] system is still used in Cincinnati as of this writing in May of 1996."

Judge Niehaus also granted a court order allowing the plaintiff's experts to "observe all phases of the election process" on election night '85. Unfortunately for the court, among Condit's experts were two brothers, Jim and Ken Collier, who arrived at the Board of Elections that night in 1985 armed with a video camera. The Collier brothers are the most outspoken and tenacious of all the activists against vote-counting fraud and have been in the fight longer than anyone else. In 1993, they released a shocking book, entitled *Votescam: The Stealing of America,* which chronicles their twenty-five year battle

against what they believe is the institutionalized disenfranchisement of the American voter [*Votescam* is available at Victoria House Press. Call 800 888-9999]

Condit told *Relevance* that the Colliers hadn't been taping long before the judge himself came down on election night wearing sneakers to "re-interpret" his own court orders at the scene, such that observing "all phases of the election process" did not include videotaping! After a heated argument, the Colliers were told to stop taping or face arrest. The brothers, who, in 1982, had videotaped members of the League of Women Voters in Dade County, Florida poking holes in punch-card ballots behind closed doors after the polls had closed, charged that Janet Reno, the then-Assistant State Attorney, had obstructed justice in that and several other instances of blatant election fraud. When Condit invited the Colliers to Cincinnati, he was amazed when they captured similar shenanigans in progress — this time Hamilton county election workers were caught using tweezers to pluck votes out of the punch-card ballots. The plausible deniability argument was that they were removing so-called "hanging chad", the official term used to describe an incompletely punched hole, however the number of holes on the floor were reportedly far beyond the few that would be expected from the miniscule "chad effect". Condit had arranged to appear with the Colliers on the Jan Mickelson radio talk show (WCKY) the next day. After local election officials refused to come on the air against the Colliers, Mickelson issued a challenge to the County Prosecutor, among others, to vigorously investigate. Mickelson's challenge was met with a deafening silence from all local public officials. Exactly one week after election day 1985, with public suspicion and outrage building, Mickelson again brought Ken Collier on his program. Less than seven hours later, both Election Supervisor Elvera Radford (a Democrat) and her assistant, Robert Uth (a Republican), simultaneously and unexpectedly announced their resignations. Radford claimed that she had planned the resignation months in advance. The demanded investigation never came.

Remote Access to Voting Computers

Included in Robert Strunk's testimony in the Cincinnatus PAC lawsuit was reference to the computers at the city's "regional computer center" (RCC) which was open to outside tampering. Strunk testified:

> Because the RCC computer system has many terminals attached to it, the vote counting system is open to alteration by parties unseen and unknown to any observers. These terminals are both local (usually within the same building) *and remote (accessed by modem over both private lines and the switched network)...*
>
> ....there is at least one staff position at the RCC which would afford someone a definite opportunity to alter the computer program that counts the ballots and, therefore, to alter the results of the election itself [Emphasis added].

Remote modem access to a central counting computer? On hearing an unconfirmed report in Michigan of a vendor representative in this month's election re-booting a computer that had "crashed" by holding a cell phone up to it, your editor popped the question to Jeff Ryan, a BRC spokesman in Chicago: could the counting computers be accessed remotely by cell phone or other device? His previously cordial tone instantly changed to a rude, insulting one. He condescendingly stated that the question betrayed a total lack of understanding of how computers actually work. Although this was not far off the mark, he still hadn't answered the question. When it was repeated, he stammered that it was a ridiculous question and seemed to want to get off the phone in a hurry, insisting that "until you go to Lynn Allen, your Oakland County Clerk and sit in his office and have him show you how the computer works, you shouldn't be asking me that kind of a question!" When he was told that he and his firm were better qualified to respond to technical questions about their own product than their politician customer, and when your editor wondered aloud why it was such a touchy question, Mr. Ryan, apparently unable to stay on the phone another second, blurted "Thank you very much, thank you —" and hung up even as the offending question was being asked for the third time.

WHY ARE MODEMS BEING PLACED INSIDE VOTING COMPUTERS?

Although we were not sure what, if anything, he was trying to hide, our curiosity was piqued, so we contacted BRC's only real competitor in Michigan, Doubleday Publishing of Kalamazoo, which sells the Accu-vote optical scanner supplied by Global Election Systems. A programming technician matter-of-factly told us that there are modems inside each of the vote-counting computers which are used to transfer results from dozens of precincts to the central counting computers. He explained, "They talk between the modems — there is a modem between each [computer] unit, or at least, most of them." Thus, the vote-counting computers can "talk" to the central computer and are, thus, technically, vulnerable to outside access. The Doubleday technician explained that special command cards can be inserted into the machine. To tell the precinct computer to call the central computer with the results, he stated:

> You have to program the phone number into the card. The card accesses the modem in the Accu-vote unit and the card tells it to dial into the central computer....To close the election you slide an "ender card" — like a special ballot — which has certain codes on it and it tells it to lock up the election.

In order to triple check this disturbing finding, we went to the State of Florida's election vendor internet website, looked under BRC and found this option available for the Optech computer vote-counter:

> Modem Communications and results transfer capability from the precinct with the OPTECH III-P Eagle and Regional accumulation with the Smart Pack Receiving system. [See also the BRC website: www.brcp.com]

The Global Election Systems' website provided further information on this innovative feature:

> At the close of the polls, the precinct results are tabulated and ready for accumulation. The Accu-Vote Tabulator has an internal modem with a pre-programmed phone number for use in transmitting precinct results.
>
> Following simple instructions, the poll workers plug a phone jack into the receptical in the back of the Accu- Vote and press a button on its front to automatically dial and transmit the precinct results to the Host Computer for county-wide accumulation.

We viewed with grave concern the presence of an internal (read *hidden*) modem which could allow outside access to the computer without anyone's knowledge. We decided to solicit the opinion of Ronnie Dugger, the author of *The New Yorker* article quoted above. Until we cited our documentation, he believed we must have been mistaken, saying, "A modem in an election computer would be highly suspect...You can't insulate a computer during vote-counting from outside communication if you have a modem in it". He granted that there may be built-in security protections, but remained concerned with the heightened danger of vote-fixing posed by an internal modem: "There could be a subroutine in the [source-code] program which would cause the results being turned into the central computer to be phoned to you too so that you could find out how many votes you needed to steal the election."

Of course, when the same company that writes the source-code, also designs the internal modem, the possibilities are endless for accessing the computer either before, during or after the election to alter or, at least interrogate, the computer's vote count. It raises the specter of a remote high-speed, vote-rigging computer automatically and surreptitiously contacting, querying and rapidly *adjusting* the votes inside many precincts and/or central counting machines nationwide.

Is this just science fiction or do we have reason to be concerned? When we shared our findings about the internal modem with *Votescam* author Jim Collier, he stated, "I think you may have found the smoking gun". *Relevance* then asked Penelope Bonsall of the Federal Elections Commission whether dangers to voting integrity could be posed by the modems in the vote-counting computers. She paused then responded: "There could potentially be a problem with that."

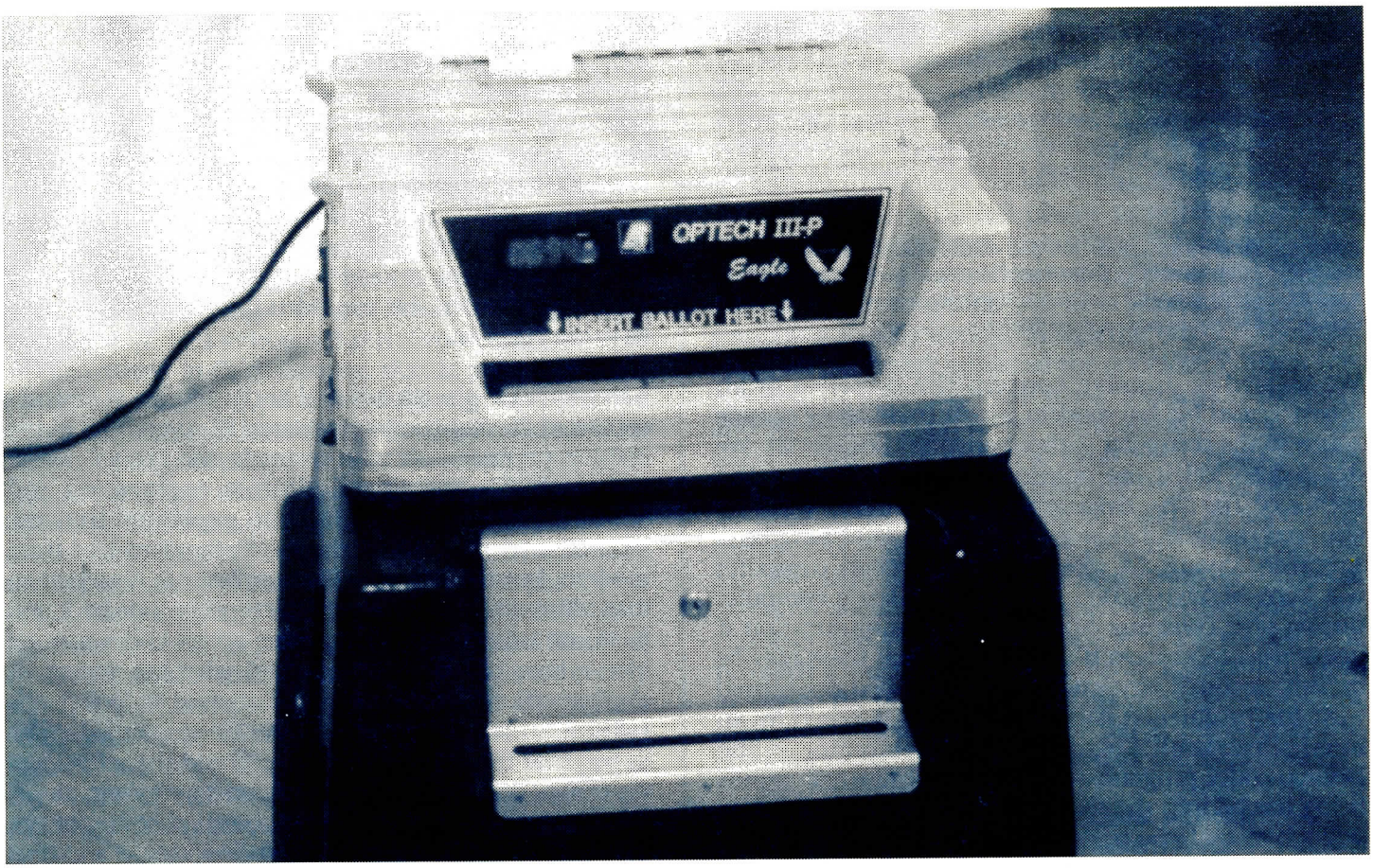
IN COMPUTER VENDORS WE TRUST?

Although it is a technically difficult subject, it is vital to know whether someone can access our vote counting computers from afar and thereby obtain election results and/or alter them. The local City of Birmingham Clerk's office could not comment on the security implications of an internal modem insisting that since the State of Michigan certified them, they must have considered potential problems. A spokesman for the Michigan Bureau of Elections was aware of the modems, but told us that they are not physically capable of allowing incoming calls, which might permit tampering with the vote totals and that the modem is not hooked up until after the polls close. When we asked about the modems inside the central counting computers at the large city and county level, he said they too "were not designed to receive incoming calls". This made no sense, since the very purpose of the internal modems is to allow the central "host" computers to receive incoming calls from the precinct computers. He conceded this point and referred us to the vendors.

After speaking with several technicians, *Relevance* contacted 25-year company veteran P.J. Lyon, one of the five top programmers who maintain the general source code at BRC's Berkeley, California engineering and manufacturing facility. Mr. Lyon explained that the internal modem is an "off-the-shelf", standard 14.4 baud modem, but that the modem's *software* is designed so that, although the machines can communicate back and forth, no one without the proper access codes can get into either computer. We asked whether voters or election officials or anyone else is allowed to look at the software to verify that it is secure. He responded, "The firmware at the remote site [precinct] and the software at the central counting facility are proprietary information." Thus, as far as the voters are concerned, whether or not the computers are secure from outside access — and thus tampering — is *unknowable.* Once again, the election is being run on the honor system and the computer vendors have the access codes to the modems. We all want to assume that they are not being sold to the highest bidders, along with "custom rigging" of the source code, but we can never really know that they're not. With all due respect to the integrity of BRC, its employees and the other vendors, that demands a degree of trust that America's 140 million registered voters *should not be required to provide.* To paraphrase Churchill: Never in the field of human politics have so many votes been entrusted by so many to so few.

IS YOUR VOTING MACHINE'S MODEM HACKER-FRIENDLY?

Lyon added that the modems, which came out a year and a half ago, are not standard in all Optech III-P Eagle computers, but because of their convenience, it is an option "that is becoming very popular" and is in use in Orange County in California and Maricopa in Arizona to name just two. Although, this is less of a concern, we asked him whether someone outside the companies and not privy to the source codes could hack into the computers via the modems? Mr. Lyon cited the numerous "checks and balances" and safeguards, but conceded, "It's certainly theoretically possible, but it has never happened, as far as we know". He also argued that, even if someone could alter the results at the central counting facility, the breech would be detected by the canvassers, since, after the unofficial results are sent out, they routinely reinsert the "PROM Paks" [see black box



Although there are no telltale phone handsets on the outside, many vote-counting machines like this one contain internal modems. We were told the modem is protected against outside access from hackers by protective software — which we cannot view because it is a trade secret. What is the protection against *inside* access by the handful of companies which are enjoying ever increasing control over the election process?

on the cover] from each precinct machine, to double check their totals against those of the central counter. Lyon stated that if these numbers disagreed with the tallies of a "rigged" central computer, the discrepancy would alert the canvassers to a problem. This makes sense, however, it assumes that the same person who hacked into the central counters did not also hack into the precinct computers, in which case there would be no discrepancy. And as we learned above, the precinct computers are equipped with standard "off-the-shelf" modems, so in answer to the above question, "Is your voting computer's modem hacker-friendly?" the truth is that you are not allowed to know, since the software that determines whether incoming calls can be made, is the company's "trade secret". The elections have been effectively *privatized.*

Also, as Mr. Dugger noted, modem access to the computers during counting could be used to find out how many votes are needed to steal the election. In the same "phone call" the election thief could then trigger a "time bomb", "trap door" or Trojan Horse waiting inside the computer's machine code (as per the Howard Strauss scenario) to start dumping the prescribed number of votes from candidate A to candidate B and the vote totals would never change. Obviously, there are many possibilities, but the central point is that, once access to the machines is compromised, the same Pandora's Box of vote-fixing tricks can be opened. If Leonard Gates was telling the truth in Cincinnati, it may have already been done 17 years ago.

There's more. The precinct computers' inaccessibility until after the polls close is based on the fact that the modems operate over standard phone lines and thus, must be hooked up to a phone jack after the voting is over. Therefore, *Relevance* asked the personable Mr. Lyon our original question: "Could the computers be accessed remotely by a cell phone or other device?" He responded, "Yes, it's possible to have cell phone access to the modems and we've tested that option here". He expects it to be offered by BRC within a year or so. Thus, despite all the checks and balances, and safeguards that may be incorporated into such a system, we might soon face the added threat of sophisticated tampering with the vote while the election is *in progress*. By extension, if the technology has already been tested, then it is possible that it has already been utilized.

THE COMPANIES THAT COUNT YOUR VOTE

Much of this discussion has centered on the fact that a small and obscure clique of election machine vendors design and service the computers which count a growing majority of our votes. While the companies themselves may be beyond reproach, their increasing power over so

many aspects of our election process, without commensurate accountability, is hardly a healthy trend. In 1993, Eva Waskell, of the Elections Project recently wrote an "Overview of Computers in Elections" in which she asked:

> Who exactly owns and runs these companies? What other businesses have they purchased? Who sits on the board of directors? Are board members affiliated with any political parties? Who are the employees? What's their background and training like? Are they United States citizens? Have they been convicted of any felonies? The public needs to be thinking about these questions. Someone needs to be providing the answers.

Relevance has learned that by far the biggest vendor in North America is Business Records Corporation (BRC) of Dallas, Texas. The company began in the sixties as Computer Election Service (C.E.S.) in Berkeley, California when IBM set up a small group of businessmen with the license to its Votomatic punch-card computer system. BRC is traded on the NASDAQ as a public company and, although it only had $150 million in revenue last year (and that included pursuits unrelated to elections), in the vote-counting industry, it is a behemoth which counts the lion's share of the U.S. vote. Since Dan McGuiness of BRC's Chicago office declined to provide *Relevance* with the company's percent of the market share (like the source-code, it is proprietary information), and since the FEC's rough estimate of 40% seemed low, we had to look elsewhere.

We were surprised to find the figure in BRC's own sales literature. According to the BRC internet website (www.brcp.com) "With approximately 60% of the market, BRC is the nation's largest provider of products and services to election jurisdictions". Although it's not clear whether this refers exclusively to voting machines, we found the figure repeated in another sales blurb: "BRC serves over 60% of the domestic market and has been a primary force in automating the nation's election processes." The firm also boasts of producing "over 100,000,000 punch card and mark sense [optical scan] ballots every year". Note that, according to FEC figures, we have approximately 140 million registered voters and only 76% of them actually vote. Thus, there were about 106 million votes cast. Although it's doubtful that all of BRC's 100 million ballots were used, it gives some sense of the magnitude of their market share. [Ed. Note: According to an FEC spokesman, the media figure of 49% voter turnout in the November election refers to "turnout of the voting age population, which includes non registered citizens"].

According to *The New Yorker*'s Dugger, Cronus Industries, (at that time BRC's parent firm) was accused by its chief competitor, the R.F. Shoup firm, of attempting to create "a virtual monopoly on the entire business of supplying voting equipment..." and of selling systems which "create new and unique opportunities for fraudulent and extremely difficult-to-detect manipulation and alterations with respect to election results." [See *The New Yorker*, November 7th, 1988, pg. 43]. When *Relevance* asked Dan McGuiness of BRC about *The New Yorker* article and the general concerns of other experts about vote-counting computer fraud, he stated:

> We don't respond to those types of articles, which are based on hearsay and are not very valid. That article is 8 years old.... it was invalid.

Of course, the R.F Shoup company was not without blemishes on its reputation. In 1979, Ransom Shoup II, the president of the firm, was convicted of conspiracy and obstruction of justice stemming from an FBI investigation of a vote-fixing scam involving the old-fashioned lever machines in Philadelphia. Mr. Shoup was fined ten thousand dollars and received a three-year suspended sentence. Thus, anyone who is offended at the mere suggestion that the vote-counting vendors could possibly be connected with vote-fixing, is referred to this case.

Foreign ownership of U.S. vote-counting?

No serious discussion of the major vote-counting companies in this country would be complete without mention of Sequoia Pacific, based in Jamestown, New York. It is the supplier of both optical scanning and direct-record computer vote-counting equipment and goes head-to-head with BRC in several regions of the country. To give some idea of its importance in the industry, the firm was recently awarded the mammoth New York City contract for its direct-record machines. *Relevance* has learned that Sequoia Pacific is owned by Jefferson Smurfit Group, p.l.c., a massive transnational conglomerate which is the largest paper-based packaging company in the world, with over 8 billion dollars per year in revenue. Jefferson Smurfit has 43,000 employees in 23 countries, including a strong presence in the U.S., which is headquartered in St. Louis. What we found most interesting is that, according to its 1995 annual report, Jefferson Smurfit is an Irish firm based in Dublin and it boasts many "heavy hitters" on its board, including Albert Reynolds, the former Prime Minister of Ireland, Ray MacSharry, a former member of the European Commission and the European Parliament; Eoin Ryan, a former Irish Senator and member of the board of the Central Bank of Ireland; a number of top Irish or European banking and air line officials, and Dr. T. A. Reynolds, Jr., a member of the board of Gannett News Services, one of the largest newspaper chains in America. This might owe in part to the fact that Jefferson Smurfit is the number four supplier of newsprint in the United States.

We asked Penelope Bonsall of the Federal Elections Commission's Office of Election Administration in Washington whether her office had concerns about foreign control of U.S. vote-counting. Without casting any aspersions on the integrity of this highly-respected firm, we questioned the propriety of such an arrangement and its implications. With so many reports of industrial espionage being perpetrated by our allies in Japan, Israel and France, to name a few, we wondered if it was wise to have a foreign firm, with unknown safeguards against criminal or foreign intelligence penetration of its computer source-code, counting the U.S. vote. She responded: "I suppose that anything is

theoretical possible but the likelihood of that happening is virtually impossible. The structure of our electoral process in this country does not lend itself to this." She was equally unconcerned about another foreign-owned company which is eyeing the U.S. vote-counting market — Computing Devices Canada.

This type of glib, yet unreassuring, response to serious questions seems to be the standard among defenders of the current computer voting system. Their trump card remains the argument that there is no evidence that there is a serious problem. Which brings us to the closest thing to a smoking gun yet to appear in the electronic voting controversy.

THE "MACHINE POLITICS" OF COMPUTER VOTING

On election night 1995 in an affluent New Orleans suburb, a few hours after the polls had closed, Republican Susan Bernecker, a popular first-time challenger for Jefferson Parrish Council, was nowhere to be found in the reported election returns. "The night of the election the numbers came in for everybody but me for an hour and a half. When my numbers didn't come in everyone in my party went wild". Later, despite major popular support for her grassroots insurgency against the Jefferson Parish machine, she went down to defeat by a 33% to 58% margin. In a recent phone interview, Bernecker told *Relevance* "In all of the 54 precincts the percentages were in the same one third/two third range — even in ones that I didn't get out and pound the pavement." She cites another female candidate in the Orleans Parrish who got 33% of the vote in every precinct. Bernecker noted that the candidate also contested her election, but the technical expert she hired wasn't allowed to examine the machines. She states that the two parishes were the only ones in the state that used Sequoia Pacific's direct-record computers.

[Editor's Note: Direct-record voting machines or DREs are the newest and most popular in the industry, but they are viewed by many to be the systems with the most potential for fraud, because there is no paper audit trail.]

After the defeat, her suspicions aroused, Bernecker and a producer friend went down to the warehouse where the Sequoia Pacific computers had been taken after the election. Demanding her right under state law to inspect the machines, she had her friend videotape her while she pressed the button next to her name on the ballot. To her dismay, the name of her primary opponent registered on a small LED located near the bottom of the machine that most voters apparently do not notice, since, according to a Sequoia Pacific official, it is two feet below the buttons. Bernecker recounts pressing her name again and again on 12 machines and she discovered that her name popped up in the LED only one out of every three times. The machine was far less fickle when her opponent's button was pressed, counting his name faithfully every time but one, when the third-place candidate's name appeared.

A WARM, IF NOT SMOKING, GUN

Bernecker, a civic activist and the owner of a fitness and health center, cried foul, along with five other candidates, who all sued the elections commissioner and the city of Baton Rouge. The judge, who, only two days before the hearing, inexplicably replaced the appointed judge (whom Bernecker considered to be fair), threw out the case the same day. She recalled, "It was a kangaroo court. What happened that day as far as I'm concerned was a joke. The tape was played but the judge was not even paying attention." Sequoia Pacific and election officials claimed that she had "rolled her finger" over onto the opponent's button, but when the tape was shown on three local news programs, "the phone began ringing right after the program" with outraged supporters who saw no such sleight of hand. Phil Foster, a regional sales manager for Sequoia Pacific, who testified before the court as a technical expert, told *Relevance*: "She would press candidate A and she would press it at such an angle that she was pushing candidate A and B's button at the same time." He called Bernecker "a sour graper".

Bernecker's tape was ultimately viewed by the New York City Board of Elections, whose Douglas Kellner opposes the direct-record machines. Another critic of computer voter machines, he agreed that rigging an election "might cost someone a million dollars worth of technology but it can be done without detection." He noted that $80 million was spent on the New York governor's race last year. Although the city of New York has signed a huge contract with Sequoia Pacific to introduce its direct-record machines throughout the city, Kellner is fighting it; "All 7,000 machines in New York City would be programmed by two people."Mr. Kellner told *Relevance* that he and the entire board had viewed Susan Bernecker's tape. When we asked him whether he thinks that she had rolled her finger or otherwise skewed the procedure, he responded: "No way. When the tape was shown to the New York City commissioners no one thought that she had rolled her finger." He added, "I think she's completely legit. The tape isn't a smoking gun, but by the very nature of this business, you can't have a smoking gun."

BULLETS AND BALLOTS

Tragically, there had been a very real smoking gun prior to Bernecker's election woes. Just two weeks before her allegedly rigged defeat, and after several weeks of harassing phone calls and death threats, she states that she was almost run off the road by a car with dark-tinted windows. After a terrifying 90 mph chase, she managed to evade her assailant. The next morning, Tony Giambelluca, the Jefferson Parish election supervisor, who was the nephew of Bernecker's opponent Nick Giambelluca, was found dead behind a dumpster with a bullet in his head. Bernecker was further stunned when there was no mention of the death in the newspapers — only two weeks from the

election. They told her that they don't normally report "suicides" unless there is something newsworthy about the case! Although she points out that Jefferson Parish City Council is the most powerful in the state — because it controls so much money — she still has no proof that Giambelluca's death had any connection to the election and the events surrounding her defeat.

CBS' "Sixty Minutes" sent a producer down for a day to get her story and she believed he was going to air it, but the program directors apparently had other ideas. Similar interest by "Prime Time Live" also fizzled. She has not yet released the tape for public distribution in the now fading hope that a national media outlet will run the story as an exclusive.

Owing in part to the local publicity from her tape last year, Republican supporters of U.S. Senate candidate Woody Jenkins, who has cried foul in his election, urged her to check the machines used in Jenkins contested defeat. Bernecker laughed as she recalled Jenkins' Senate race: with only ten minutes left in the count, and losing by a few thousand votes, Jenkins' opponent suddenly surged ahead with ten thousand votes that came out of the predominantly inner city Orleans parish, which had been noted for low voter turnouts. But, in her local paper it was said to have enjoyed a turnout of 105%! Bernecker and associates went to the Orleans parish and attempted to obtain vote total printouts from the backs of the 800-plus machines, but their count was inexplicably halted by local officials after they had counted only 80 machines. It seems that, for Susan Bernecker and New Orleans area voters, getting a little justice in the Big Easy is a difficult thing.

What of skeptics who have a hard time believing in the kind of conspiracy that would likely be required to rig the national vote? Eva Waskell pointed out that we could never have illicit drug conspiracies without people everywhere along the chain from producer to smuggler to pusher, to money launderer to corrupt cop, etc., all willing to break the law for profit. Could the same kind of corruption grow up over the years around the election process? Now, more than ever, elections at every level are high stakes, big business, with candidates and special interests' campaign expenditures running into the *billions* each year. Are these "honorable men" beyond reproach? We've all seen dozens of venal congressmen and hundreds of greedy local politicians going to jail on bribery and influence-pedaling convictions, and our last two issues of *Relevance* carefully documented evidence of almost unimaginable corruption at the highest levels of government. Jim Collier, the author of *Votescam*, appearing on WXYT's Mark Scott show recently observed, "people complain that they can't find an honest car mechanic and that their lawyer is ripping them off and their butcher has his thumb on the scale, but they somehow put their faith in politicians, who are the biggest crooks in America, thinking 'Oh no, these big Washington power brokers would *never* rig an election'". As we've shown, computer vote fraud is not only feasible but, by its very nature, undetectable. And by our election officials' own admission, no cases of computer vote fraud have ever been successfully prosecuted. Thus, it is hard to conceive of an organized criminal enterprise with such a favorable combination of high profit potential and low risk.

WHAT CAN BE DONE?

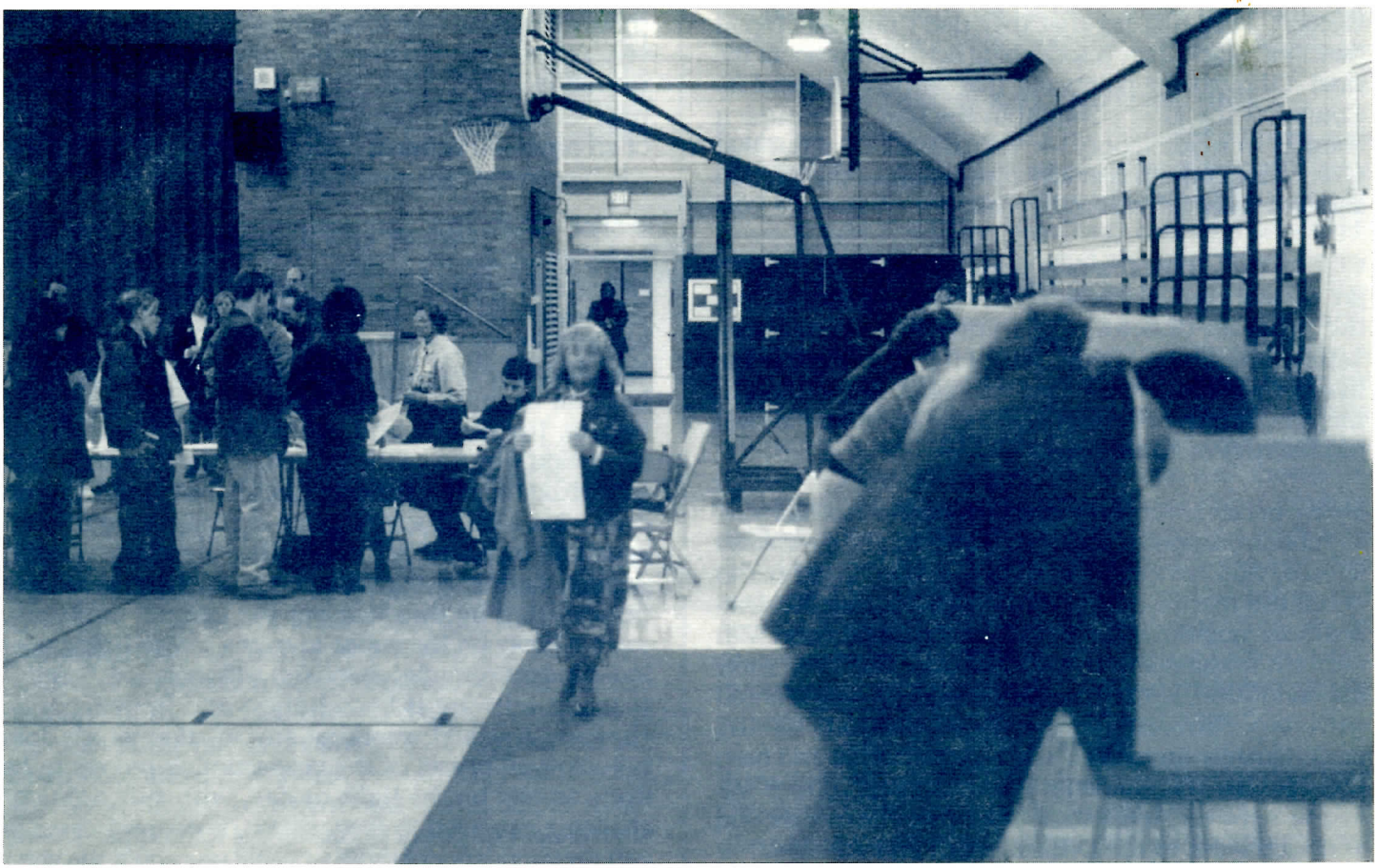
Roy Saltman, one of the true experts in this field, recently made a candid admission to *Relevance*: "I've been trying to make improvements in this system for 20 years and have failed." What has hampered his efforts? He and a handful of others have fought against bureaucratic inertia, ineptitude and probably a fair amount of corruption with very little support. As the Illinois election official lamented, "Nobody cared". For those who do care, what kind of solutions are available to rectify this appalling problem? Although there are many possible ways of shoring up the sieve of computer voting security (we can start by throwing out the internal modems!), most still rely on the public to trust a few technicians or independent commissioners who will somehow "certify" that the software is both honest and impenetrable. However, it would seem that any solution which does not allow all phases of the vote-counting process to be done in the bright light of day, with full rights of challenge extended to every citizen, is doomed never to win the confidence of those who still care about the vote.

The grassroots activists led by Jim Condit and the Collier brothers back a return to hand-counting, in which young and old turn out en masse in each community to challenge the voters, count the votes and publicly post the results at every stage. Jim Collier notes that this is how elections are still run today in Israel and India, the world's largest democracy. Even P.J. Lyon, the BRC programmer, offered, "I would like to see more manual recounts, because it would increase confidence in the process." Roy Saltman reasons that mandatory handcounts of a certain percentage of all races (as was instituted in West Virginia after its voting scandal) would be enough to prevent most computer vote fraud. Although many would lampoon handcounts as a "neo-Luddite" return to the days of the horse and buggy, would it not be a step up from our current status as trusting techno-chumps who have no idea if Pandora's black box is telling the truth?

[Editor's Note: Those interested in getting involved in this issue are strongly urged to visit Jim Condit's website (www.networkusa.org) and to write to the Precincts Project Institute, P.O. Box 11339, Cincinnati, OH 45211].

Coming December 1996, *Relevance* explores the missle theory in the downing of TWA Flight 800.

This 2nd edition of the November 1996 issue of *Relevance* is a special offer to supporters of Citizens for a Fair Vote Count. See back cover for special subscription offer.



If more Americans knew the truth about electronic voting, and its secret source-codes, hidden modems, and suspicious outcomes, they might give the current system a decisive vote of no confidence.

"WHENEVER A MAN
HAS CAST HIS EYE ON OFFICE,
A ROTTENNESS BEGINS
IN HIS CHARACTER."

JEFFERSON

RELEVANCE
Publisher:
Relevance Corporation

Editor:
Philip M. O'Halloran

Associate Editor:
Charles Bennett

Business and editorial correspondence:
Relevance Corporation
320 E. Maple Rd., Suite 297
Birmingham, MI
48009-9894