Whistleblower Stephen Heller faces years in prison for exposing voting machine manufacturer Diebold’s possible criminal activities.

Los Angeles Daily Journal reports that Alameda County spent nearly $12 million in taxpayer dollars on Diebold machines that were ultimately unable to serve their intended purpose. (Alameda County was awarded $100,000 as part of the settlement mentioned earlier.) In San Diego, where Diebold’s machines also malfunctioned, some 40,000 people were reportedly unable to cast their vote, disenfranchised by Diebold because there was no Plan B in place when machines malfunctioned.

The thanks Heller got for speaking up and trying to protect Americans’ votes was a full-slate smear campaign designed to ruin his life and send a clear signal to any other prospective whistleblowers.

The Oakland Tribune published several of Heller’s smoking-gun Jones Day memos after receiving them from activists working with BlackBoxVoting.org. The Tribune reported that Jones Day counsel McMillan told prosecutors he was distraught over the incident.

“He now has a hard time trusting others,” the D.A.’s investigators wrote in a report. “McMillan’s 20-year legal career is in jeopardy due to the act of the criminal [Heller] who was working at Jones Day.” McMillan claimed Heller endangered his posh legal job by making him look bad to his clients, who were understandably upset that their attorneys were unable to keep confidential information secure.

Many see this so-called criminal as a hero. Heller detractors point to the attorney-client privilege, a sacrosanct bond. After all, having “whistleblower” on your résumé is not a big draw for prospective employers. Criminal prosecution is another matter.

The California Whistleblower Protection Act §1102.5 states: “An employer may not make, adopt or enforce any rule, regulation or policy preventing an employer or employee from disclosing information to a government or law-enforcement agency, where the employer or employee has reasonable cause to believe that the information discloses a violation of state or federal statute, or a violation or noncompliance with a state or federal rule or regulation.”

The California Whistleblower Protection Act §8547.1 further stipulates: “The Legislature finds and declares that state employees should be free to report waste, fraud, abuse of authority, violation of law or threat to public health or safety without fear of retribution.”

Yet the 44-year-old Heller now faces criminal prosecution because “whistleblower status” only protects one from retribution by employers. Criminal prosecution is a bigger matter entirely. Little did Heller know that powerful forces were working against him.

Heller first learned he was under investigation early one morning in August 2004, when a contingent of police officers and investigators showed up at his home with a search warrant. Eighteen months elapsed before the perjury charges were finally brought against him in February 2006. The L.A. County District Attorney’s office charged Heller with felony access to computer data, receiving stolen property and commercial burglary. Heller has pleaded not guilty.

According to a blog written by Heller’s wife, Michele Gregory, during the search, officials confiscated the couple’s belongings, such as cell phones, computers and address books—even Gregory’s favorite shoes. (She and her husband were unable to speak to us on the record while the case was ongoing.)

“You have to have a sense of humor when your world is crumbling all around you, and you can’t seem to stop it,” she wrote.

“I couldn’t believe it,” Stephen Heller told The Oakland Tribune about the raid. “I thought it must be a mistake… I kept thinking they had the wrong house, that they were after someone else…. It was just very frightening; it was so surreal.”

Federal and state authorities declined to prosecute Heller, but the L.A. County District Attorney’s Office was still too happy to catch this “thief,” who, by all accounts, had never even been a political activist.

Now, as Heller fights to regain control of his life, Diebold machines continue to fail everywhere in the country. In December 2005 its optical-scan systems were hacked in a mock-election test in Leon County, Florida. The results were flipped without a trace. Diebold would eventually admit that its software contained code banned by federal Voting System Standards. It was this code the hackers had exploited. As of this writing, the banned code has still not been purged.

Shortly after the Leon County simulated hack, an independent study commissioned by California’s new Secretary of State, Bruce McPherson, a Diebold supporter at the time, found another 16 bugs in just one portion of Diebold’s voting system. The analysis described the bugs as a “more dangerous family of bugs ever reported.”
In March 2006 Bruce Funk—a county clerk in Emery County, Utah—allowed independent computer security experts to inspect Diebold’s newest line of touch-screen voting machines. Not surprisingly, the experts found new security vulnerabilities that surpassed what had been found previously. The stunning new vulnerabilities have been described by computer scientists and security experts as “the nuclear bomb for E-voting systems” and “the most serious security breach that’s ever been discovered in a voting system.”

Funk, who held his elected position for 23 years, has been forced out by Diebold and state officials. BlackBoxVoting.org is currently providing funds for legal support as Funk battles to retain his job.

BlackBoxVoting.org described these latest discoveries in Utah as “a major national security risk.” The revelation eventually led Pennsylvania to lock down and sequester all Diebold touch-screen machines just days before the May 2006 primary elections. Caught off guard, voting officials scrambled to find a solution.

The defect is said to be extremely severe, affecting every Diebold touch-screen voting machine in the country. It was unclear at press time if the flaw—which could allow a malicious individual to completely overwrite the software without a password—will ever be remedied. A solution would require a complete reinstallation of all firmware and software on every machine.

Diebold purposefully built this high-security risk “feature” into its voting machines for “easier updates,” but apparently the company never thought it noteworthy to alert officials. Even after the problem was revealed in Utah, it failed to notify the state of Ohio, which was about to use the very same machines just weeks later in 41 counties as part of the 2006 primary elections. Cuyahoga County was eventually plagued with failing Diebold tabulators, the malfunction resulting in some 17,000 absentee ballots having to be counted by hand.

The corrupt, untrustworthy Diebold is now using Heller’s case to send a clear message: Fuck with us; pay the price.

Luckily, election-integrity advocates continue to take a stand. BlackBoxVoting.org and other groups—notably VoteTrustUSA.org, VotersUnite.org and VelvetRevolution.us (all of whom have minimal resources and little more than the truth on their side)—maintain the faint glimmer of hope that democracy might be restored in the United States. For the courageous Stephen Hellers out there, saving America from tyranny is what it’s all about.

The gravest irony in this matter is that if Stephen Heller is convicted of any one of the three pending charges, even if handed a suspended sentence due to his having no prior criminal record, as a felon he would be stripped of his right to vote.

And may God bless America.

For additional information, or to assist the beleaguered whistleblower financially, visit HellerLegalDefenseFund.com.