DEVELOPMENTS—
TRADE SECRET

JENNINGS V. ELECTIONS CANVASSING COMM'N

No. 2006-CA-2973, 2006 WL 5508548 (Fla. Cir. Ct. Dec. 29, 2006), cert. denied, 958 So. 2d 1083 (Fla. Dist. Ct. App. 2007)

In *Jennings*, a Florida appeals court denied certiorari with respect to a trial court's non-final order denying a request to compel disclosure of trade secrets, including the source code and other proprietary technology associated with voting machines.

In the November 2006 congressional elections, Republican candidate Vern Buchanan won Florida's 13th congressional district over Democratic candidate Christine Jennings by less than 400 votes. High undervote rates cast doubts on the electronic voting technology utilized and the election result. About fifteen percent of the total ballots cast in the district did not include a vote in the race between Jennings and Buchanan. In contrast, neighboring districts that used regular paper ballots reported only a two percent undervote rate.

Jennings and eleven voters filed suit in state court, filing a motion to compel expedited discovery which asked Election Systems & Software, Inc., makers of the voting machines, to disclose trade secrets, such as the source code for the election software and other proprietary voting machine technology. The trial court denied the request for the source code, dismissing plaintiffs' expert testimony as conjectural and speculative, and finding no basis to rule that plaintiffs' access to the code was "reasonably necessary" where, the court stated, granting access "would result in destroying or at least gutting the protections afforded those who own the trade secrets."

The Court of Appeal for Florida, First District, denied Jennings' petition for a writ of certiorari. The appeals court noted that orders denying discovery are generally not reviewable because such errors can be rectified on plenary appeal. Jennings did not meet the burden of demonstrating that "the trial court departed from the essential requirements of law, resulting in irreparable, material injury for the remaining trial proceedings that cannot be rectified on direct appeal."

Proponents of electronic voting emphasize the accessibility and increased political participation facilitated by machines that can accommodate multiple languages and offer audio capabilities. Those concerned about electronic voting worry about the reliability of the hardware and software of electronic voting machines, the obstacles to a meaningful recount posed by unverifiable votes cast in exclusively digital format, and the danger of hackers manipulating the results. Lending weight to these concerns, a recent report by the University of California testing California's electronic voting systems found that "the security mechanisms provided for all systems analyzed were inadequate to ensure accuracy and integrity of the election results and of the systems that provide those results." However, a separate study suggested that the undervote in the 13th district may have resulted from poor ballot design on the voting interface, rather than voting machine malfunction or security problems. When, as in *Jennings*, competing theories are offered to explain an undervote, an examination of voting machine source code could provide evidence as to the actual cause. However, as *Jennings* illustrates, the presence of trade secrets—coupled with the difficulty of appealing discovery orders—may create a significant obstacle to the prompt resolution of voting disputes.