

Managing the Web Electorate

Software glitches muddy the outcomes of electronic elections

D is d. Or is it? Susan Desbarats, a favored candidate in a Calgary region's first elected board, was surprised to find she was trailing her rival, Athena d'Arras, by hundreds of votes during an October election. However, well after defeat was conceded and many supporters had gone home, a campaign worker noticed that Desbarats had actually won the race.

Blame for the mix-up was placed squarely on a computer glitch that had assigned the wrong totals to each candidate. The glitch arose when the database that sorted the election's votes tallied many of them according to the letter "D" for Desbarats, but also "d" for d'Arras, her opponent's surname.

On the other side of the globe, Australia's first election that offered electronic voting met with some unexpected delays due to what was referred to as "technical hiccups." What essentially amounted to an overloaded Web site resulted in a near standstill in vote counting.

"We're getting lots of hits on our Internet site and that's actually slowing down our server," ACT Electoral Commissioner Phil Green explained during the count. Though accuracy wasn't a point of contention, the load issues that slowed down the collating process are sure to be recurring ones.

Any Web testers interested in a job in Australian government?

—from [Canada.com](#)
and [Computerworld.com](#)



“This increase in the prominence of the thumb is basically a case of people evolving with technology.” —So says Sadie Plant, who's head of a new study at Warwick University that proves the thumb is the most dexterous digit thanks to a generation raised on cell phones and handheld computer games.

Snow White Isn't So Pure

Two new DVDs bring more tears than laughter

The Powerpuff Girls inadvertently hatched a plan that would make Mojo Jojo—their evil monkey nemesis—proud. It seems their recently released *Meet the Beat Alls* DVD is the first ever to spread a virus to those who download the disc to a computer (DVD players are unaffected). The virus, known as "FunLove," is an oldie-but-goodie after two years in existence. It's also No. 7 on the Top 10 list of infectious code.

Three programs on the disc, including the installer, are able to wreak havoc on a network via any hard drives shared with the infected system.

But the Powerpuffs aren't the only entertainment divas who've had trouble making the transition to DVD. Disney's *Snow White and the Seven Dwarfs* DVD has proved glitchy with thousands of Windows XP and Windows 2000 operating system users.

According to Microsoft spokesman Greg Sullivan, Disney "didn't test the disk on Windows 2000 or Windows XP." This oversight caused a number of consumers to experience playability failures and receive error messages when they tried to view the DVD.

—from [BBC News](#) and [CNET News.com](#)

Information Anarchy Rages On

When it comes to software vulnerabilities, the question remains: to tell or not to tell?

It happened to Yahoo. It happened to America Online. It happened to Microsoft. Each of these major players in the technology game has had one (or more) major vulnerabilities re-

vealed to the world by hackers. One thing blamed for repeated attacks on these weak spots is a practice favored by some security experts called "full disclosure," a custom that allows for the publishing of as much information as possible about any vulnerability.

"It's high time the security community stopped providing blueprints for these weapons," Scott Culp, manager of the Microsoft Security Response Center, explains. "We can and should discuss security vulnerabil-

ities, but we should be smart, prudent, and responsible in the way we do it."

But a hacker group called the Nomad Mobile Research Center (NMRC) believes that by quashing this information anarchy, much of the information will simply go underground. The result may then be that the *only* ones who will have information about vulnerabilities are the hackers themselves.

Some feel full disclosure is a benefit as long as it's not made public, but others feel that by not making it public, vendors will be "tempted to brush vulnerabilities under the carpet."

The debate was once again fueled last November when two computer science doctoral students developed programs that allowed them to hack into the IBM 4758, the computer that received the U.S. government's highest tamper-resistance rating in 1998.

"A crooked bank manager could duplicate our work on a Monday and be off to Bermuda by Wednesday afternoon," says Richard Clayton, one of the students.

The two students have since posted copies of their programs to the Internet.

—from [Reuters](#), [ZDNet.com](#),
and [vnet.com](#)