TUESDAY, SEPTEMBER 11, 2001 LOS ANGELES TIMES

Are Judges Soft on Snooping?

By BART KOSKO

Judges have allowed privacy invasions in many public and private forums. Now it may be the judges' turn to lose some digital privacy.

Just look around. There are more police cameras at traffic lights, public parks and buildings. More private surveillance cameras in shopping malls, grocery stores and hotels. More companies that build and swap customers' digital profiles and that track Internet users' "clickstreams" as users visit Web sites and chat rooms.

And a new study from the Privacy Foundation found that 14 million workers—a full third of the online work force—"have their Internet or e-mail use under continuous surveillance" and that the main reason for this is that surveillance software is so cheap. Another study found that as many as 72% of employers sometimes read their employees' e-mail.

The U.S. Supreme Court has repeatedly said that we should expect less privacy in public places. This applies to the phone numbers we dial and the addresses we write on envelopes and the trash cans we set out.

And, believe it or not, the 4th Amendment's noble prohibition on unreasonable searches and seizures does not apply to private companies if there is no governmental conduct involved.

The founding fathers missed that one.

But the judges' main argument to permit the explosion in digital surveillance comes down to three words: Use equals consent.

Staying is playing. Don't drive or shop or visit Web sites if you don't want others to see what you do and to record it. And don't work at a company if you don't want to give up your digital privacy.

> "Use equals consent" should not be the guide.

So even many longtime workers must now "consent" to their company's latest policy of electronic surveillance if they want to keep their jobs. The U.S. Supreme Court has not yet ruled on employee Internet surveillance, but it has upheld the dubious wiretap rule of the "unreliable ear": You assume the risk that everyone you speak to has consented to letting the government wire them to record what you say.

That lays a nice foundation for a surveillance state.

Supreme Court Chief Justice William H. Rehnquist will head the U.S. Judicial Conference, the policymaking body for federal judges and staff, when that panel of federal judges meets in Washington today to vote on a controversial proposal to monitor the e-mail and Internet access of the 30,000 employees of the federal judiciary (although growing criticism may lead to a vote postponement).

A subcommittee of the Judicial Conference unanimously approved a report last month that recommends that the government continue its new practice of monitoring the e-mail and Internet access of federal judges and their staffs. But the report recommends that each computer screen display a notice that states that the "use of the system constitutes consent to such viewing and recording." Earlier monitoring found that a few employees had downloaded porn, music and streaming video.

Many prominent judges have sharply criticized the proposal. Fifth Circuit Court of Appeals Judge Edith Jones sent the report's chief author a letter stating that the proposed policy is "the equivalent of sanctioning wiretapping of telephones or searches of office files to prevent unauthorized use of government property."

Judge Alex Kozinski of the 9th Circuit Court of Appeals published an open letter to the Judicial Conference warning that the new surveillance could undermine judicial independence: "I had assumed that keeping case deliberations confidential was a bedrock principle of our judicial system."

The 9th Circuit shut down the e-spy software for a week in May to protest its use. But why shouldn't judges suffer the same loss of digital privacy as the rest of us?

One reason is that this may be the only way to set a precedent that favors employee privacy. Simple fairness will at least make it morally harder for judges to deny the same e-privacy to non-judges.

The California Legislature has failed to secure such privacy. In August, the state Assembly passed Sen. Debra Bowen's right-to-know bill (SB 147), which would require employers to tell their employees when the company monitors their e-mail, just as employers must now tell their employees if they monitor their phone calls.

But Gov. Gray Davis vetoed a similar bill a year ago and is likely to veto the Bowen bill.

Another reason judges shouldn't suffer a loss of digital privacy is that e-privacy protects ju[illegible] independence.

The FBI or political pa[illegible]s could use the e-monitor da[illegible] U.S. Senate confirmation hea[illegible]. The FBI could even use the data to pressure suspect judges when the FBI seeks a warrant for an arrest or wiretap.

Think of the mischief that J. Edgar Hoover could have caused with access to such a spy system.

Perhaps the best reason to support judicial privacy is pragmatic: More than water flows downhill. If judges vote to do this to themselves and give up their own electronic privacy, then just think what they will let others do to the rest of us.

Bart Kosko, the author of "Heaven in a Chip" (Random House, 2000), is on USC's electrical engineering faculty.