UNITED STATES COURT OF APPEALS
FIFTH CIRCUIT

HONORABLE EDITH H. JONES
12505 U.S. COURTHOUSE
515 RUSK AVENUE
HOUSTON, TEXAS 77002-2655

PHONE: [713] 250-5484
FAX: [713] 250-5017

August 18, 2001

Honorable Edwin L. Nelson
Chairman, CAT Committee
786 Hugo L. Black United States Courthouse
1729 Fifth Ave. N.
Birmingham, ALA 35203

Re: Comments on the Report of the Committee on Automation and Technology

Dear Judge Nelson:

Chief Judge King has sought comments on the report to the Judicial Conference by the Committee on Automation and Technology (CAT Committee), concerning Internet and computer use policies for the judiciary. I am pleased to respond. I hope my criticisms will be viewed as reflecting constructive ideas that the Committee should integrate into a reconsideration of its recommendations.

Some of the Committee's working principles regarding Internet usage cannot be gainsaid. For instance, unwanted intrusions into the judiciary's computer network must be prevented. Inappropriate use of government property should be discouraged and, if found out, punished. The work of the judiciary should not be compromised from either external or internal Internet misuse.

The Committee's report, however, wholly ignores other principles: the judges' position as chiefs, not subordinates within the judicial branch; judges' responsibility and prerogative to manage our own chambers; legitimate privacy concerns; the inevitable overlap and symbiosis between private business and judicial business; and the desirability of less intrusive means to achieve the Committee's aims.

As I read the CAT Committee's report, it does nothing to alleviate the concerns that prompted me and nearly every other member of my court to criticize the monitoring program that the Administrative Office imposed last spring. We objected to the

following features of that program, which I shall explain in layman's terms:

(1) While purporting to survey only excessive Internet bandwidth usage, the program in fact had the capability to snoop into the content of the judiciary's computer transmissions.

(2) The program did not distinguish judicial chambers from other offices within the judiciary and so enabled snooping directly into judges' personal communications.

(3) Although we were told this would not occur, the program enabled snooping into e-mail as well as other types of Internet usage.

(4) The program was at some point and continues to be operated by outside contract employees, creating a potential security breach as well as compromising the confidentiality of computer usage within the courts.

(5) The program was ordered and directed from Washington without prior knowledge of or notice to or consultation with any but a very few judges.

(6) Finally, the Internet monitoring was neither revealed to all the judges at the time it was undertaken, nor was its operation satisfactorily and fully explained after the fact.

Perhaps the CAT Committee was unaware of these concerns when it formulated its recent recommendations. I believe those recommendations simply do not respond to most of the above concerns. If anything, they perpetuate the problems in the previous, unannounced monitoring program.*

First, the recommendations continue to centralize decisionmaking about Internet and computer usage policy in the Administrative Office and, perhaps, in unspecified committees or persons within the Judicial Conference. This seems contrary to a longstanding trend toward decentralized court management. Moreover, while they are ambiguous, these recommendations appear to confer enormous discretion on the judicial bureaucracy to continue monitoring communications and to make policy decisions regarding

---

* A caveat to my remarks is in order. The Committee Report states that no monitoring of Internet signatures will occur through December, 2001 unless authorized to counter a threat to judiciary computers from outside the system. Further, several programs will be blocked because of their propensity to permit tunnels that can be used by hackers. I do not criticize these measures, but as I read the report, the Committee may well recommend a resumption of monitoring after its December meeting. I write for the purpose of discouraging that next step.

Internet and computer use that each judge should make for his or her chambers.

Second, the emphasized rationale for centralization is to furnish a nationwide minimum level of protection from unwarranted intrusions by outside hackers. This is certainly an acceptable goal. But the Committee Report conflates external threats and internal possibilities of misuse, and its recommendations plainly contemplate novel, invasive and extraordinary monitoring of computer use within the judiciary. The recommendations would advise judicial branch employees that no one, including judges, has any expectation of privacy in his use of government computers for Internet or e-mail purposes. This is the equivalent of sanctioning wiretapping of telephones or searches of office files to "prevent unauthorized use of government property."**

Third, no one condones using government computers to download pornography, to gamble, to conduct personal profitmaking business during office hours, or to achieve illegal or immoral goals. But to subject every judicial employee to random snooping and wiretapping of Internet communications is a drastic measure that should only be justified by proof of the most serious and systemic misuse. The Committee report adduces no such proof; the report refers to no more than a few dozen examples of misuse among the thousands of judicial branch employees. Moreover, one may question how many breaches of innocent employees' privacy were committed to uncover these few abuses. It seems highly disproportionate to inflict a monitoring program that may invade thousands of peoples' privacy for the sake of exposing a handful of miscreants.

Fourth, the Committee's report does not explain why alternate, less intrusive measures to discourage Internet or computer misuse within the judiciary are impractical. For instance, in March, after the monitoring program became publicized, the Executive Committee issued a communique regarding appropriate usage that was widely disseminated throughout the judiciary. We have been told that bandwidth usage immediately and dramatically declined in response to that communique. If exhortation is sufficient to discourage inappropriate use, why undertake random snooping? Moreover, I'm sure we all know specific instances in which inappropriate computer use has been detected on the local level and appropriately disciplined in the absence of monitoring. Why is it assumed that local, decentralized policing will be ineffective? Finally, the demands of hierarchy, longstanding

---

** For the sake of brevity, I am not analyzing each aspect of the Committee Report that seems to me questionable. But I am especially concerned that the general policies expressed in Attachment D suggest an unprecedented intrusion into the management of judges' chambers and that what is fitting for the Executive Branch is not so for the Judiciary.

custom and common sense suggest that judges ought to decide autonomously on the appropriate types of Internet and computer use for their individual chambers. Why does the CAT Committee think judges' independent decisionmaking is inadequate in this area?

Fifth, the Committee report and recommendations do not forestall the use of the private contractors, who are still involved in intrusion detection, in a renewed monitoring effort. Thus, it is possible not only that judicial bureaucrats will be monitoring computer traffic in judges' chambers, but that individuals with no links or loyalty to the judiciary will also be able to do this. It is no answer to say that the "monitoring" takes place on the broad level of bandwidth usage. The technology employed for that purpose may just as easily be used to inspect the substance of communications. If this were not so, why would the proposed monitoring policy expressly say that there is no expectation of privacy in these communications?

In conclusion, I have no doubt that the CAT Committee was well motivated, but I think their recommendations bespeak a solution in search of a problem. The recommendations are grossly disproportionate to any demonstrated need for monitoring Internet and computer communications within the judiciary. The recommendations do not take account of legitimate privacy interests and foreordain a workplace in which suspicion and paranoia may become rampant. Not the least of my concerns is also that judges' autonomy is being sacrificed to some paternalistic ideal generated from who-knows-where in Washington, D.C.

I suggest that the Committee step back from these recommendations, take a deep breath, and recall that one of the first principles of leadership is to foster trust and mutual respect among one's team members. In an organization like the federal judiciary, with our highly trained, well-educated employees, surely we can expect more of ourselves and our team members than these benighted privacy-invading recommendations imply.

Very truly yours,

Edith H. Jones

Edith H. Jones

EHJ/rh
cc: Chief Judge Carolyn D. King