JUDICIAL CONFERENCE OF THE UNITED STATES
COMMITTEE ON INFORMATION TECHNOLOGY

May 10, 2002

Honorable Howard Coble
Chairman, Subcommittee on Courts,
the Internet, and Intellectual Property
Committee on the Judiciary
United States House of Representatives
B351A Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

I understand that on May 2, 2002, the Judiciary Subcommittee on Courts, the Internet, and Intellectual Property held a business meeting to consider H.R. 4125, the "Federal Courts Improvement Act." At the meeting Mr. Berman first offered and then withdrew an amendment relating to "monitoring" of electronic communications on the judicial branch's Data Communications Network (the "DCN"). I am told that Mr. Berman may again offer his amendment when H.R. 4125 is considered by the full committee. Those of us who serve on the Judicial Conference Committee on Information Technology (the "IT Committee") believe the proposed amendment would constitute an unwarranted and unneeded intrusion into the internal workings of the Third Branch and would, in fact, cause substantial harm to the judiciary's ongoing automation efforts.

As you are aware, the work of the Judicial Conference of the United States is supported and facilitated by the work of 24 committees, the members being appointed by the Chief Justice of the United States who serves as the presiding officer of the Judicial Conference. The IT Committee, formerly the Committee on Automation and

Technology, which I chair, is comprised of 14 judges–one from each of the regional circuits, one magistrate judge and one bankruptcy judge. The IT Committee is responsible for providing policy recommendations to the Judicial Conference on its subject-matter jurisdiction, planning, and oversight of the judiciary's many automation programs.

I am told Mr. Berman expressed some concern that on two occasions, in 1998 and 2000, Administrative Office (the "AO") personnel may have monitored or blocked Internet communications on the DCN. In 1998, the AO was not involved at all and the action in 2000 was directed by the IT Committee.

During the early spring of 1998, at the direction of the Ninth Circuit Council, the Ninth Circuit technical staff installed and activated at the Ninth Circuit Internet gateway a filtering software system called WebSense, with the goal being to determine access through that gateway to adult-oriented materials by DCN users in the Ninth Circuit. AO personnel were not involved.

Findings by Ninth Circuit staff which resulted from the short-term use of WebSense are revealing. On April 28, 1998, Ninth Circuit technical staff reported to the then chief judge of that circuit that a local review by staff of that court of logs over a 28-day period revealed that users in the three circuits served by that gateway had accessed approximately 1100 "adult" web sites approximately 90,000 times. Two explanatory notes may put those figures in better perspective. While 90,000 "adult" site accesses may seem high, one must remember that every click on a new link, even at one site, will be recorded as a separate access. On the other hand, 3.6% of total accesses may not seem particularly high, but if one remembers that "adult" sites tend to be graphics and media intensive, the actual traffic generated by those accesses was probably higher than 3.6% of the total traffic, up to 40% to 50% of available bandwidth.

That staffer attached to his memorandum to his chief judge a 7 page "partial listing" of some 300 "adult" sites that had been accessed. An examination of the names of sites shown on the list suggests that transfers of files to or from many such sites would likely violate federal law prohibiting the sexual exploitation of children. Some such names–ones that I can repeat here were: allteens.com; cyberteens.com; hotteen.com; hotteensex.com; and hollywoodteens.com.

As a result of the findings of the filtering, the Circuit determined to block access to adult-oriented sites. Placement and removal of WebSense on the Ninth Circuit Gateway were decisions taken by appropriate authorities in the Ninth Circuit.

At its meeting in January 1999, the IT Committee recommended to the full Judicial Conference, that it authorize the AO to install software at each of the national gateways to block access to adult-oriented, pornographic Internet web sites. At its meeting in March 1999, the Judicial Conference declined to accept that recommendation, believing that such blocking was a matter more appropriately addressed by each court. Subsequently, the Ninth Circuit stopped blocking.

At its meeting in December 2000, the IT Committee was informed that demand for bandwidth (capacity) on the DCN for access to the Internet had almost doubled over the preceding 10 months. Several members of the committee had received anecdotal complaints and the AO had received numerous specific complaints about slow access to and responses from the Internet. Concerned that IT resources purchased with tax payer funds be used appropriately, the IT Committee directed committee staff from the AO to determine the cause of the increased demand and to report to the committee at its meeting in June 2001.

Responding to the committee request, in January 2001, AO personnel activated two filters or "signatures" on the already installed and operating intrusion detection software at the three national gateways to identify high volume files passing through those gateways. Experience has taught us that music and movie files tend to be among the largest on the Internet. One twenty-second video/movie clip may be the equivalent of sending two thousand pages of typed text. Signatures activated on the intrusion detection software were intended to detect and log the passage of such large files. The logging consisted of recording several items of data: (1) the date and time; (2) the IP address inside the DCN; (3) the IP address outside the DCN; and (4) the name of the file passing through the gateway. The user inside the DCN could not be identified because the AO has no way to do that. It can only identify the judiciary facility to which any IP address has been assigned. The information captured showed that a substantial portion of Internet traffic was non-business related and that a few judiciary users were engaged in extraordinarily high volume downloading of music and movies. Many of the Internet site and video file names suggested they contained pornography. Others suggested they might contain depictions of children engaged in sexually explicit conduct, prohibited by federal law. Finally, many were music files that were most likely copyrighted.

Let me emphasize again that neither the Director of the AO, nor the employees of the AO, nor the IT Committee members knew then or know today, the identities of any DCN users who were involved with this downloading. Only local IT staff, operating under the direction of local judges, have the ability to determine the identity of any user

of the DCN. Moreover, this so-called "monitoring" captured the content of video and music files only to extent that the web site and file names suggested such content.

Use of the "offending" intrusion detection signatures was discontinued in early June 2001 after the Executive Committee of the Ninth Circuit Judicial Council unilaterally, and without notice to either the Eight or Tenth Circuits, directed its technical staff to disable all aspects of the intrusion detection system at the Ninth Circuit gateway. Reasonable people may disagree about the serious level of risk created by this action but it is clear that the intrusion detection system was, and is, an integral part of the DCN security apparatus and that simply "turning it off" exposed DCN users in the Eighth, Ninth, and Tenth Circuits, and perhaps throughout the entire federal judiciary, to considerable risks to the security of their electronically stored data and electronic communications and, indeed, to their privacy interests.

The intrusion detection software was reactivated in a short time, but only without the music and movie signatures as demanded by the Ninth Circuit Council.

In a special meeting on July 27, 2001, the IT Committee recommended to the Judicial Conference that it adopt on an interim basis the Internet appropriate use policy developed by the Federal Chief Information Officers Council of the General Services Administration. Excluded from that recommendation was a provision of the executive policy which sought to define and limit privacy interests of executive officers and employees. In a mail ballot following its shortened meeting of September 11, 2001, the Conference accepted the IT Committee recommendation.

In the interim, the IT Committee has developed controls that allow the AO to change intrusion detection signatures at the national gateways only in certain specified circumstances. For example, the AO may respond to emergency situations as they arise by adding needed security signatures but such signatures may remain in place for no more than 14 days without the explicit approval of the committee chair or his designee. The need for this emergency response authority was demonstrated in late October and early November 2001 when the DCN was hard hit by the NimdaE email virus.

At least four significant factors counsel against the adoption of this amendment:

- It represents the sort of micro management of judiciary affairs that would seriously threaten the independence of the Third Branch and of the many judges, both Article III and Article I, who serve in that branch.

- It would seriously impair the ability of the courts to administer and manage its wide area network–the foundation on which many of the courts' information technology programs depend. For example, the courts are rapidly developing and implementing modern and robust case management systems that will provide the ability to create and maintain electronic case files. A new and modern technologically advanced financial accounting system that will permit the courts to better manage and account for appropriated funds is being deployed. Both these and other projects require a technologically advanced and secure wide area network.

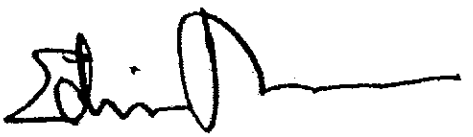
- Under the present state of the law, the federal judiciary is governed by the provisions of the Electronic Communications Privacy Act (the "ECPA"). This amendment would, in my opinion, call into question the status of the judiciary under the ECPA, while leaving intact provisions of law that allow other government and private entities to protect their IT infrastructures and their users. It is unclear to me why the federal courts, with exceptionally higher interests in the security and integrity of the information that is created, transmitted, and stored on court systems than many others, should be afforded less protection than are they.

- There is no articulated need for the proposed amendment. Instead, the Judicial Conference and its Committee on Information Technology are fully engaged in addressing these issues and have demonstrated that they are sensitive to the privacy and security needs of judges and judiciary employees. As judges we are quite capable of considering all sides of virtually any issue, weighing the competing interests, and striking appropriate balances between them. That is what judges do.

Finally, let me debunk a misconception that seemingly gained acceptance among some judges last year. There is not now; there has never been; and there are no plans ever to "monitor" judiciary email. We just last week completed the implementation of the Lotus Notes email system throughout almost virtually all of the entire federal judiciary. Judiciary users now have the capability to encrypt any piece of email to any other judiciary user so it can be read only by the intended recipient. We are investigating the means by which we can provide similar encryption capabilities for email going to or coming from the Internet.

If you or any members of your committee have any additional concerns or questions, I will be pleased to answer them, either by phone, mail, *encrypted* email, or, if you prefer, in person.

Sincerely,



Edwin Nelson
Chairman, Committee on
Information Technology

cc: Members of the Judiciary Subcommittee
on Courts, the Internet, and Intellectual Property
Members of the Judicial Conference Committee
on Information Technology