SANAIS
433 North Camden Drive
#600
Beverly Hills CA 90210
Tel. 310-717-9840
Email: cyrus@sanaislaw.com

July 24, 2018

BY OVERNIGHT MAIL, EMAIL AND HAND DELIVERY

Hon. Charles Grassley
Chairman, Senate Committee on the Judiciary
135 Hart Senate Office Building
Washington, D.C. 20510

Hon. Dianne Feinstein
Ranking Member, Senate Committee
on the Judiciary
11111 Santa Monica Blvd., Suite 915
Los Angeles, CA 90025

Re: Confronting Sexual Harassment and Other Workplace Misconduct in the Federal Judiciary

Nomination of the Hon. Brett Kavanaugh to the United States Supreme Court

Dear Senators Grassley and Feinstein:

I am writing to you in your respective capacities as Chairman and Ranking Member of the Senate Judiciary Committee. The purpose of this letter is to urge an immediate follow-up hearing to the June 13, 2018 hearing on "Confronting Sexual Harassment and Other Workplace Misconduct in the Federal Judiciary." The June 13, 2018 hearing was substantially insufficient, because it failed to call witnesses to address the institutionalized policies of retaliation against employees of the courts, law clerks, and third parties who expose judicial misconduct. This issue needs to be addressed now because there are persons who work for, or who have worked for, the federal judiciary who have important stories to tell about disgraced former Chief Judge Alex Kozinski, and his mentee, current United States Supreme Court nominee Brett Kavanaugh.

I know that there are people who wish to speak out but fear retaliation because I have been contacted by more than a half-dozen such persons since Judge Kozinski resigned in disgrace. I am a California attorney and non-practicing English solicitor based in Beverly Hills. I was contacted because. along with former Ninth Circuit Executive Greg Walters and former head of the Administrative Office of the Courts L. Ralph Mecham, I was a victim of retaliation by Judge Kozinski and the Ninth Circuit Judicial Council for standing up to or exposing Judge Kozinski's misconduct.

Everyone who has worked for an extended period of time for the federal judiciary knows the story, but no one wants to come out and say it. Nobody believes that the proposed reforms to the

federal judiciary's procedures will be effective, because nobody believes that a whistleblower or complainant will be shielded from retaliation, or that any kind of meaningful investigation will be done.

In order to create a safe space for such persons to come forward, the Senate Judiciary Committee (and House Judiciary Committee, should it choose to get involved) should issue subpoenas and call witnesses to expose the two-decade long history of cover-ups, judicial retaliation and plain old head-in-the-sand willful blindness that allowed Judge Kozinski's sexual and workplace harassment and other misconduct to flourish since the beginning of the millennium. Moreover, the judges who were at the forefront of protecting Kozinski were "liberal lions" such as the late Stephen Reinhardt, former Chief Judge of the Ninth Circuit Mary Schroeder, and current Chief Judge Sidney Thomas. Such exposure, and a plan to root out Judge Kozinski's enablers, will give the persons hesitant to come forward sufficient confidence that they will not suffer the same punishment as Mr. Walters, Mr. Mechem and myself for telling their stories.

Judge Kozinski's Sexual Deviancy and his Combat with Walters and Meachem

The Ninth Circuit was aware as early as 1998 that it had a significant and ever growing problem involving employees of the federal judiciary using government-owned computers to download pornography.[1] One judge, Alex Kozinski, fought to preserve the freedom of the judiciary to use taxpayer-funded money to visit "www.zoosex.com". As far back as 1998 he questioned the proposed solution: implementation of an Internet monitoring program. The United Judicial Judicial Conference took responsibility for this program and implemented a monitoring system that showed significant and increasing downloading of music and video files, some of which the late Judge Edwin Nelson believed included child pornography.[2]

In 2001 the monitoring system was disabled unilaterally in San Francisco. Who did this is a matter of dispute. Mr. Mecham accuses Judge Kozinski of taking this action personally and that this constituted criminal activity,[3] while the late Judge Nelson ascribed it to the Ninth Circuit's executive committee acting unilaterally,[4] while Judge Sidney Thomas claimed in an article that the entire Ninth Circuit Judicial Council unanimously approved the action. Whichever the case, Judge Kozinski was the moving force behind this action. Mr. Mecham's direct knowledge of this issue strongly suggests that the Ninth Circuit acted to shield Judge Kozinski from his misconduct. Even if the Ninth Circuit's Judicial Council or Executive Committee did approve what Judge Kozinski did, it is undisputed that the 11th Circuit and 10th Circuit had no idea this was being done; more important, if the motivation of the action was to allow de facto unfettered

[1] *See* Exhibit 1 hereto (memo from Greg Walters, Circuit Executive). It should be noted that the seven page list of URLs attached to the memo is one quarter of the sites visited by Ninth Circuit computers during the on-month survey period.
[2] *See* Exhibit 5 hereto, E. Nelson, Letter to Hon. Howard Coble, May 10, 2002, at 3. I received a copy of this letter from Mr. Mecham.
[3] *See* Exhibit 2 hereto, a memorandum from Mr. Mecham. He also filed judicial misconduct complaints against Judge Kozinski.
[4] Exhibit 4 at 4.

access to pornography by crippling the monitoring system, then the action was wrongful no matter how many judges approved it.

Judge Kozinski, apparently losing the internal battle on this issue, published an article in the Wall Street Journal on September 2001 directly attacking Mr. Mecham by name.[5] In that article Judge Kozinski represented to the world the following:

> The policy Judge Nelson[6] seeks to defend as benign and innocuous would radically transform how the federal courts operate. At the heart of the policy is a warning--very much like that given to federal prisoners--that every employee must surrender privacy as a condition of using common office equipment. Like prisoners, judicial employees must acknowledge that, by using this equipment, their "consent to monitoring and recording is implied with or without cause." Judicial opinions, memoranda to colleagues, phone calls to your proctologist, faxes to your bank, e-mails to your law clerks, prescriptions you fill online--you must agree that bureaucrats are entitled to monitor and record them all.
>
> This is not how the federal judiciary conducts its business. For us, confidentiality is inviolable. No one else--not even a higher court--has access to internal case communications, drafts or votes. Like most judges, I had assumed that keeping case deliberations confidential was a bedrock principle of our judicial system. But under the proposed policy, every federal judge will have to agree that court communications can be monitored and recorded, if some court administrator thinks he has a good enough reason for doing so.
> Another one of our bedrock principles has been trust in our employees. I take pride in saying that we have the finest work force of any organization in the country; our employees show loyalty and dedication seldom seen in private enterprise, much less in a government agency. It is with their help--and only because of their help--that we are able to keep abreast of crushing caseloads that at times threaten to overwhelm us. But loyalty and dedication wilt in the face of mistrust. The proposed policy tells our 30,000 dedicated employees that we trust them so little that we must monitor all their communications just to make sure they are not wasting their work day cruising the Internet.
>
> How did we get to the point of even considering such a draconian policy? Is there evidence that judicial employees massively abuse Internet access? Judge Nelson's memo suggests there is, but if you read the fine print you will see that this is not the case.
>
> Even accepting the dubious worst-case statistics, only about 3% to 7% of Internet traffic is non-work related.

[5] Exhibit 3.
[6] This is the same Judge Nelson who authored the letter attached as Exhibit 4.

Judge Kozinski's representations were dishonest in several respects. First, and perhaps most important, it has never been the case that federal judicial deliberations have "inviolable" confidentiality; the confidentiality is, under the law, far more violable than, say, the attorney-client privilege. Indeed, this is precisely the contention he forced into his clerk's brain to stop them from complaining about his sexual harassment of them.

Second, Judge Kozinski represented to the world that there was no problem involving use of the Internet by employees of the judiciary. That is simply a lie, as made clear by the 1998 Walters memorandum[7] and the 2002 letter of Judge Nelson.[8]

Kozinski's retaliation against Mecham through the press was not his only method of striking back. When Kozinski became the Chief Judge, he fired Greg Walters, the author of the memorandum attached as Exhibit 1 and the person who attempted to dam the flood of pornography into the Ninth Circuit, and replaced him with the then-sitting clerk of the Ninth Circuit, Cathy Catterson. Catterson had pledged her loyalty to Kozinski, so she was allowed to keep her other job as well. Catterson became Kozinski's enforcer inside and outside the Ninth Circuit, ensuring that no one in the judiciary's staff would raise any complaints about Kozinski's bizarre antics.

While Kozinski succeeded in keeping free access to pornography, his battle with the judicial administration had educated him about the realities of Internet network technology. The systems then being installed in the federal judiciary kept detailed records (for purposes of network security and tracing hackers) of every website accessed by any computer on the Ninth Circuit's network and the computer accessing it. While Kozinski disabled the centralized monitoring from Washington D.C., the logs could be accessed at any time. This left Kozinski's habitual porn-surfing at risk of constant exposure. He therefore hit on the plan of transferring his favored pornography and other material he liked to distribute to a personal server on the alex.kozinski.com server on the kozinski.com domain that he had purchased.

Kozinski placed on this server material that he wished to distribute or view in chambers. Rather than sending copies of documents, audio files, or audio-visual files, he could simply send a link by email. If someone was viewing a pornographic video on his server within the court (including Judge Kozinski himself), the network log would show access to a file on alex.kozinski.com, and not accessing a file on www.zoosex.com or any of the other sites that it amused Kozinski to view and to make his clerks view.

"Kozinski Strikes Back" at Me.

I submitted an opinion piece to *The Recorder* of San Francisco concerning the ongoing controversy over citation of unpublished opinions.[9] In his opinion piece, I argued that the critics

[7] *See* Exhibit 1.
[8] *See* Exhibit 4.
[9] C. Sanai, *Taking the Kozinski Challenge,* The Recorder*,* September 16, 2005

of the Ninth Circuit's policy regarding publication had a legitimate argument concerning the dedication of the Circuit to consistent precedent. This issue was about to be decided by the Judicial Conference, then-proposed (and now adopted) Federal Rule of Appellate Procedure 32.1. Judge Kozinski's testimony to Congress on this subject was cited by me as representing the view of those opposing citation of unpublished opinions. I also urged the Court to grant more rehearings en banc to settle perceived or actual conflicts in Ninth Circuit authority, starting with the conflicts surrounding the Court's *Rooker-Feldman* precedent.

It was while researching Judge Kozinski's views on the subject of citation of unpublished appellate dispositions that I first came across alex.kozinski.com, specifically the directory alex.kozinski.com/articles/. There were numerous links discoverable by Google to articles in this directory, some of which had clearly been supplied by Judge Kozinski himself.

Four days after my was published, the Judicial Conference decided the issue in favor of permitting citations. Judge Kozinski was quoted condemning this move by the Judicial Conference, and expressing his hope that the Supreme Court would reject it.[10]

Two days later, Judge Kozinski published his response to Complainant's article in *The Recorder,* which stated, *inter alia,* that he had recused himself from then pending cases involving my family in which I was a litigant.[11] Judge Kozinski laid out a response to the arguments in the pending petition and a novel analysis of the Ninth Circuit's past precedent concerning the *Rooker-Feldman* doctrine.

Judge Kozinski's article did not address the primary subject of my article, which is the citation policy of the Ninth Circuit. It ignored my discussion of the debate between the majority and dissent over what constitutes binding precedent in the Ninth Circuit.[12] It did not dispute my contention that as a practical matter, the Ninth Circuit's recent *Rooker-Feldman* authority operated to erase the injunctive remedy against biased or corrupt state court judges and tribunals authorized by the United States Supreme Court.[13] Instead, Judge Kozinski focused the first part of his article solely on refuting my contentions that there is a severe conflict in the Ninth Circuit's authority concerning the *Rooker-Feldman* doctrine. He began the second part of his article as follows:

> Despite his colorful language, Mr. Sanai's article raises no legitimate question about whether the Ninth Circuit has been derelict in following circuit or Supreme Court precedent. But the article does raise serious issues of a different sort. Mr. Sanai's article urges us to "grant en banc rehearing of the next decision, published or unpublished, which asks the court to resolve the split among *H.C., Napolitano*

[10] Tony Mauro, *Cites to Unpublished Opinions Ok'd,* Legal Times, September 21, 2005
[11] Alex Kozinski, *Kozinski Strikes Back,* The Recorder, September 23, 2005.
[12] *See Barapind v. Enomoto,* 400 F.3d 740, 751 fn. 8 (9th Cir. 2005)(en banc)
[13] *Compare Gibson v. Berryhill*, 411 U.S. 564 (1973) *with Flangas v. State Bar of Nevada,* 655 F.2d 946 (9th Cir. 1981).

> and *Mothershed*." A petition for en banc rehearing raising this very issue crossed my desk just as Mr. Sanai's article appeared in print. The name of the case? *Sanai v. Sanai.* A mere coincidence of names? Not hardly. The petition, signed by Mr. Sanai, cites the same cases and makes the same arguments as his article — including the reference to "Catch-22."

Kozinski Strikes Back, supra.

Judge Kozinski placed case-related documents on his personal website, www.alex.kozinski.com, and had the web version of his article link to the .pdf file of the selection of these documents on his website.

Canon 3(A)(6)[14] of the Code of Conduct for United States Judges then in effect stated that "a judge should avoid public comment on the merits of a pending or impending action." The official comment further states that "[t]he admonition against public comment about the merits of a pending or impending action continues until completion of the appellate process. If the public comment involves a case from the judge's own court, particular care should be taken that the comment does not denigrate public confidence in the integrity and impartiality of the judiciary."

Judge Kozinski's move from impartial judge to public advocate of my opponent's legal position while a petition for rehearing en banc is pending has no precedent in federal legal history.

[14] The D.C. Circuit had the opportunity to address Canon 3(A)(6) when it chastised District Court Judge Jackson in the Microsoft antitrust trial. That court noted:

> While some of the Code's Canons frequently generate questions about their application, others are straightforward and easily understood. Canon 3A(6) is an example of the latter. In forbidding federal judges to comment publicly "on the merits of a pending or impending action," Canon 3A(6) applies to cases pending before any court, state or federal, trial or appellate. *See* Jeffrey M. Shaman et al., Judicial Conduct and Ethics § 10.34, at 353 (3d ed. 2000). As "impending" indicates, the prohibition begins even before a case enters the court system, when there is reason to believe a case may be filed. Cf. E. Wayne Thode, Reporter's Notes to Code of Judicial Conduct 54 (1973). An action remains "pending" until "completion of the appellate process." Code of Conduct Canon 3A(6) cmt.; Comm. on Codes of Conduct, Adv. Op. No. 55 (1998).
>
> ....
>
> It is no excuse that the Judge may have intended to "educate" the public about the case or to rebut "public misperceptions" purportedly caused by the parties. [Citation.] If those were his intentions, he could have addressed the factual and legal issues as he saw them — and thought the public should see them — in his Findings of Fact, Conclusions of Law, Final Judgment, or in a written opinion. Or he could have held his tongue until all appeals were concluded.

U.S. v. Microsoft Corp., 253 F.3d 34, 113 (D.C. Cir. 2001).

Though Judge Kozinski has recused himself from voting on the petition for rehearing en banc that I filed, it is clear that he was not refraining from taking an active, public and vocal role to influence the outcome of the petition or the ultimate disposition of the case, formulating new interpretations of the Ninth Circuit's case law that have never seen the light of day and which I had no opportunity to address. Any reasonable person would find that his actions "denigrate public confidence in the integrity and impartiality of the judiciary", by setting a precedent whereby a sitting judge may recuse himself and then adopt the role of public advocate for one side concerning a pending petition for rehearing en banc arising from interlocutory appeals.

I filed a judicial misconduct complaint against Judge Kozinski in October of 2005. The order concerning the complaint was issued on December 19, 2006, more than 14 months later. It terminated the complaint on the grounds (a) that corrective action had been taken as to Judge Kozinski's publication in the Recorder, and (b) there was no evidence of any website controlled by Judge Kozinski which held such materials.

Both determination were false. Judge Kozinski has never "apologized" to me at all. There is no evidence of any such apology ever being made by Judge Kozinski in any fashion.

More important, Judge Schroeder's finding that there was no website containing posting by Alex Kozinski was, as we know, completely untrue. She delayed the resolution of the complaint with Judge Kozinski to convince him to disconnect the server and because *The Recorder* and law.com site makes its web-based articles available for a period of one year, then erases them. Accordingly, the Kozinski article and the link to the .pdf files he had published were no longer accessible on the law.com in December of 2006.

But while the links disappeared, I had .pdf copies of the original online article and some of the documents which had been linked, and I had submitted those with petition to review Judge Schroeder's order, which was denied by the Judicial Council with its form order.

Sometime in 2007, Judge Kozinski concluded that it was safe to reactivate the alex.kozinski.com website. He therefore brought the site back on-line and began distributing links to the portion of the site which includes his articles, including a .pdf scan of the paper version of the "Kozinski Strikes Back" article. The act of distributing links to other sites results in search engines such as Google locating and indexing alex.kozinski.com. Google indexed the portion of alex.kozinski.com containing a hyperlink to the "Kozinski Strikes Back" article.

I filed a second judicial misconduct complaint in November of 2007 regarding Judge Kozinski's redistribution of "Kozinski Strikes Back". Judge Kozinski, now chief judge, assigned the matter to Judge Schroeder, who, true to form, sat on it.

The more I thought about the treatment of Judge Kozinski's alex.kozinski.com site, the more puzzled I became. Why did Judge Schroeder pretend the site did not exist? Why did Judge Kozinski take the site down, then put it back up? Why did Judge Kozinski believe that he could redistribute the "Kozinski Strikes Back" article with impunity?

On the night before 2007's Christmas Eve, after putting my children to sleep with tales of the excitement of the next day, I decided to find out what Judge Kozinski might be distributing via alex.kozinski.com website. On December 23, 2007 and December 26, 2007 I discovered the stuff index containing Kozinski's distributed porn, mp3's and other documents, and I downloaded as much as I could before Judge Kozinski shut the site down. I checked the site on January 10, 2008 and downloaded one music file.

Realizing that I had found the reason Judge Kozinski and the Ninth Circuit Judicial Council refused to acknowledge the existence of the alex.kozinski.com site, I first sought to have the story published under my own name. I passed the information to John Roemer of the Daily Journal. His David Huston killed the story, and may have tipped above Kozinski. Terry Carter of the ABA Journal began working on it. When I read the article about Judge Kozinski presiding over an obscenity trial, I tipped the Los Angeles Times. The Los Angeles Times reporter Scott Glover independently accessed the site and apparently found files and documents that had been placed in the directory after I had done my downloading and thus saw documents that I never saw. Judge Kozinski recused himself from the Ira Isaacs trial, leading to an ongoing battle over whether double jeopardy applied.

More important, Judge Kozinski filed a judicial misconduct complaint against himself. This stratagem put Judge Kozinski in effective control over the prosecution of the misconduct complaint for purpose of appeals. The Ninth Circuit entered an order in respect of the complaint initiated by Judge Kozinski against himself that "[a]ny pending complaints, or new complaints that may be filed, relating to this matter are included in this request for transfer" to a different Circuit, which Justice Roberts selected as the Third Circuit. However, when I filed my own complaint directly with the Third Circuit, it was rejected, and when I filed a complaint with the Ninth Circuit, instead of transferring it, it was stayed, in direct violation of Court's own order.

The Third Circuit's investigation of Judge Kozinski, led by its Chief Judge Sirica, was a joke. No competent computer expert was officially hired to investigate the server. The persons who had viewed the contents, myself and Scott Glover, were never called as witnesses. The two law firms selected to do the legwork on the investigation, Morgan Lewis and Dechert, were the two Philadelphia-based firms that had offices in California and regularly litigated before the Ninth Circuit, and thus would have a conflict of interest if Kozinski were offended by aggressive investigation. The only witness called was Kozinski himself. Though I submitted an affidavit to the Third Circuit investigators, not a single question was ever put to me, and evidence I presented to show that the server was used to distribute pornography within the Ninth Circuit was ignored.

Judge Kozinski was effectively reprimanded by the Third Circuit. Had the Third Circuit performed an even marginally competent investigation, it would have interviewed his clerks; his clerk in 2007, Heidi Bond, was forced to watch pornography by Kozinski and would likely have revealed what she knew. But rather than make the obvious inquiry into why Judge Kozinski was placing pornography and other materials on his server, the Third Circuit only listened to him and

found his explanation, including his statement that he never showed these materials to anyone else, "credible." Bond has stated that she separately ask advice from Judge Sirica about how to complain about Judge Kozinski, and Sirica, who has headed the Judicial Misconduct appellate body of the Judicial Conference, said he could not tell her what to do.

"Liberal Lion" Stephen Reinhardt Initiates Punishment Against Me

Soon after the Third Circuit issued its ruling, my complaint, against Kozinski and other judges involved in the matters he wrote about, was handed to Kozinski's best friend on the Ninth Circuit, so-called "Liberal Lion" Stephen Reinhardt. Reinhardt found that every matter I raised (including internal distribution of pornography within the Ninth Circuit) had been thoroughly investigated and that Judge Kozinski had been found innocent. He also found that I should be sanctioned, and an order to show cause demanding that I explain why I should not be sanctioned for, among other things, revealing the contents of my complaint, was issued by the Judicial Counsel. I was reprimanded and the Judicial Council instructed Catterson to seek my disbarment in 2010.

The California State Bar reviewed the California State Bar complaint, and explained to Catterson in a letter I was given in 2014 that unless it released a copy of the judicial misconduct complaint I filed and provided other information, it could not prove a case against me. This did not discourage Catterson from continuing to pressure the Bar. Jayne Kim,[15] the then-newly appointed Chief Trial Counsel of the California State Bar Association, overruled prior Chief Trial Counsels and instigated proceeding against me as requested by the Ninth Circuit Judicial Council and regarding another case where Judge Kozinski had teamed up with a judge I reversed, disqualified, and whose nomination to the Court of Appeal I opposed sought to punish me. The Judicial Council refused to provide any records concerning my complaints against federal judges and refused to allow anyone from the federal courts to testify. When I sought to subpoena Catterson, the actual complainant, Kozinski, and other judges to defend myself, they refused to show up.

After presentation of the Chief Trial Counsel's case in 2014, in 2015 the California State Bar Court dismissed the charge, finding that to the extent that it could determine the contents of a misconduct complaint filed by me against Kozinski and others, it was justified.[16] The State Bar Court judge later wrote that:

[15] Kim subsequently was subject of a no-confidence vote by her trial counsel underlings and was accused of misconduct by the man who recruited her, former state legislator and former executive director of the State Bar Joseph Dunn. Dunn was fired, and he lost an arbitration. D. Walters, "Joe Dunn loses arbitration over his firing by State Bar", Sacramento Bee, March 20-21, 2017. Kim resigned in 2016.

[16] At the end of the State Bar Prosecutor's case I won on all but one charge, and the remaining charge has been stayed for three years because it will require state court judges to testify. I have never been allowed to put on a defense.

> Given the State Bar's inability to provide this court with a copy of the actual complaints filed by Respondent against the federal judges, this court - as accurately predicted by the State Bar in May 2011 -eventually dismissed that count at trial due to the State Bar's failure to provide clear and convincing evidence that those complaints were frivolous. The evidence was not sufficient even to enable this court to identify all of the judges against whom complaints had been filed.

Catterson's non-stop pressure on the State Bar, to prosecute a case that the Ninth Circuit refused to supply documents necessary to win the case, was the epitome of bad faith harassment. It was conducted by the members of the Judicial Council to ensure that no outsider would ever make complaints against Judge Kozinski, and served as a stark warning to anyone within the Court about the lengths that the Council would go to in order to punish anyone who embarrassed Kozinski.

Kozinski's Luck Runs out with #MeToo

During my ordeal with Judge Kozinski, I learned that it is impossible to have legal beat reporters initiate investigative work against judges, and that many editors will kill stories involving the judiciary because of the desire to keep access. No one has exploited this more assiduously than Kozinski. My efforts to expose him at the Daily Journal and Slate were killed by David Houston and Dalia Lithwick, respectively. Lithwick subsequently gave a partial mea culpa, admitting that her reluctance to expose Kozinski was due in part because she feared being cut-off from lucrative speaking engagements.[17]

Kozinski's luck ran out when a national security reporter for the Washington Post, Matt Zapotosky, hunted down clerks and judges who reported on the open secret of Kozinski's sexual harassment of clerks and even other judges. After defending himself to another friendly reporter, Maura Dolan of the Los Angeles Times, a second group stepped forward and Zapowsky published even more damaging revelations, so Kozinski resigned. The exposure of this open secret led Justice Roberts to establish the working group whose work was the subject last month's hearing.

During this time period I was contacted by more than half a dozen clerks, former clerks, employees and former employees of the federal judiciary. Half of Zapowsky's sources refused to identify themselves because of fear of retaliation, and there are other people who want to come forward with stories about Judges Kozinski, Reinhardt, Kavanaugh and possibly others. However, they are rightly terrified of doing so because of the punishment meted out by the Ninth Circuit Judicial Council against Walters, Mecham and myself, and the whitewashing of Kozinksi's misconduct by Judge Sirica and the Third Circuit Judicial Council.

[17] D. Lithwick, "He Made Us All Victims and Accomplices, Slate, Dec. 13, 2017

The only way these important stories can be told is if Congress moves the spotlight from abstract procedures and statements of intent to the judges who made the judiciary safe for Judge Kozinski to satisfy his deviant needs. If this Committee, or the Judiciary Committee, does so, I have assurances that more people will step forward.

Kozinski and Kavanaugh

The need to address this problem now was highlighted by Zapotosky's most recent article published on July 24, 2018, "Judge who quit over harassment allegations reemerges, dismaying those who accused him." The Washington Post article discusses the efforts to rehabilitate Kozinski by his friends in the press such as David Houston, and the concerns his reemergence have raised in those trying to reform the judicial workplace. The article stated that:

> "I worry that it signals to women that our profession doesn't actually care about harassment," said Emily Murphy, a law professor who was among the first to describe her experience with Kozinski on the record. "And it substantiates a concern that several of us had after he resigned — that in the absence of an investigation or formal process, it would be easier to downplay his conduct and rehabilitate him from something we never got to the bottom of."
>
> The timing of Kozinski's reemergence is notable, coming just as Kennedy retired and Trump nominated Kavanaugh to replace him. In recent weeks, opposition researchers and journalists have been exploring Kozinski and Kavanaugh's relationship, trying to determine whether Kavanaugh knew of his former boss's conduct. Kavanaugh clerked for Kozinski in the early 1990s, and the two men both vetted candidates for Kennedy clerkships. One of Kozinski's sons worked as a clerk for Kavanaugh last summer.

Though Kozinski is off the bench, the judges who protected him, such as Schroeder, Thomas, and Sirica, are still there. The majority of the judges who served on the Ninth Circuit Judicial Council from 2001 to date are also still judges. Their conduct merits investigation and if appropriate, impeachment and removal from the bench. This needs to be done now, to give individuals who have important stories to tell the safety to tell them without retaliation by the Judicial Council.

This Committee should do the following:

1. Subpoena all Judicial Council records and intra Court emails and messages relating the judicial misconduct complaints filed against Kozinski by myself, Kozinski, and Mecham.
2. Subpoena all intra Court emails and messages between Kavanaugh and Kozinski and all emails to and from Kozinski with links to his website.
3. Subpoena all records, particularly emails to and from Cathy Catterson, regarding the bar complaint made by the Judicial Council against me.

4. Publicly release all material obtained from the subpoena
5. Immediately call a hearing with at least the following witnesses:
    a. Myself;
    b. Greg Walters (if he is willing to speak);
    c. L. Ralph Mecham;
    d. Judge Mary Schroeder;
    e. Judge Sidney Thomas;
    f. Judge Anthony Sirica;
    g. Cathy Catterson.

Exposing the protectors of Kozinski will encourage others to come forward, and is a prerequisite to meaningful reform in the federal judiciary.

Kavanaugh, Partisanship and Me

I have no direct, personal knowledge that Judge Kavanaugh is either qualified or disqualified to be appointed to the United States Supreme Court, and I have no position at this time. I do have two observations about Zapotosky's discussion of concerns about Kozinski and Kavanaugh in his July 24, 2018 article.

First, if Judge Kavanaugh states that he never heard or observed anything that would suggest that Judge Kozinski behaved inappropriately, he is either lying or so willfully blind to judicial misconduct that he should not be appointed. Everyone knew, even if everyone did not have personal knowledge.

Second, assuming Kavanaugh did hear rumors or observe Kozinski's pervy public behavior, I have no idea what Kavanaugh could have done that would have been effective to stop Kozinski. Kavanaugh became a federal judge in 2006 and I exposed Kozinski in 2008. The Ninth and Third Circuit Judicial Council, including the Ninth Circuit's "liberal lions," closed ranks to protect Kozinski and directly retaliated against anyone who crossed Kozinski. Under the federal judicial disciplinary system, Kozinski was the Ninth Circuit Judicial Council's responsibility, and until #metoo, there was nothing Kozinski could do that would cause the Ninth Circuit Judicial Council to cease protecting him or forbear from striking back at his accusers. When a misconduct proceeding was sent to the Third Circuit, Kozinski was given the gentlest and most effective whitewash the judiciary could muster. Even if Kozinski had been tried again, he likely would have gotten off by offering yet another apology.

My demand for an investigation crosses partisan interests. The strong connection between Judges Kavanaugh and Kozinski merits immediate initiation of an investigation, and obviously this could delay, or even destroy, Kavanaugh's nomination if there is evidence that he was an enabler of Kozinski, or Kavanaugh is misleading about what he knew. However, Kozinski's strongest bodyguards, and the ones most deserving of removal from the bench, are and were "liberal lions," including the first female chief judge of the Ninth Circuit.

Until Congress acts, there will be no protection for whistleblowers or judicial employees like Mecham or Walters who stand up for the interests of the judiciary against errant judges. Congress should act now to expose Kozinski's enablers and allow people to come forward with whatever additional information they have about Kozinski and his judicial "family," including Judge Kavanaugh.

Very truly yours,

Cyrus Sanai

Exhs. 1-4 attached.

cc: Hon. Kamala Harris (with Exhibits)
Hon. Richard Blumenthal (with Exhibits)
Hon. Bob Goodlatte (without Exhibits)
Hon. Jim Sensenbrenner (without Exhibits)
Hon. Jerry Nadler (without Exhibits)
Hon. Ted Lieu (without Exhibits)

EXHIBIT 1

Office of the Circuit Executive

UNITED STATES COURTS FOR THE NINTH CIRCUIT

95 Seventh StreetGregory B. Walters, Circuit Executive
Post Office Box 193939Phone: (415) 556-6100
San Francisco, CA 94119-3939Fax: (415) 556-6179

---

to: Judicial Council

from: Greg Walters, *Circuit Executive*

date: April 23, 1998

re: Internet Access to Pornographic Material

Judge Kozinski's memo (attached) raises a question about the management of the Internet Project that requires your attention. In a nutshell, the question before you is whether we should continue to block access to pornographic sites on the Internet for the Judges and Staff of the Ninth Circuit.

Background of the Internet Project

At its September 1997 session, the U. S. Judicial Conference approved a judiciary-wide policy regarding access to the Internet from computers connected to the DCN. The policy requires access to the Internet be provided only through national gateway connections approved by the Administrative Office pursuant to procedures adopted by the Committee on Automation and Technology of the USJC. (See IRM bulletin 97-19, attached)

The Office of the Circuit Executive for the Ninth Circuit maintains one of these three national Internet gateways from the judiciary's internal data communications network (DCN). The Administrative Office and the Fifth Circuit maintain the other two gateways. Our office provides Internet services to approximately 10,000 users in the Eight, Ninth and Tenth circuits.

The determination of the location of the gateways was based on considerations of geography as well as personnel expertise and infrastructure at the sites.

The Internet access project was established for three purposes:

1. To provide Internet access to members of the Judiciary,
2. To provide in-bound and out-bound Internet e-mail services,

3. To provide website hosting services for court units and assist in development and implementation of such sites.

The decision to limit the number of gateways to three was made to preserve the integrity of Data Communications Network (DCN). The security of the entire judiciary's network relies on properly maintained firewalls at the gateways. The fewer access points, the better the security. Rather than allowing each court unit in the United States to provide independent access to the Internet, the USJC Committee on Automation and Technology determined that all Internet traffic should flow through one of these three sites thus dramatically reducing the potential for security intrusions. A firewall is usually a computer and software that sits between an internal network (the DCN) and the Internet, monitors all traffic and and only allows authorized traffic to traverse the firewall.

After a thorough review of the available options, the three gateways agreed upon standard hardware and software configurations. The products that were put in place were Firewall-1 and WebSense. Firewall-1 is the most widely used firewall product. It offers high-level security without decreasing the performance of the network. Firewall-1 logs every Internet transaction, both in-bound and out-bound, for security purposes. The logs are highly detailed, including date, time, Internet address of user, site accessed, and protocol used.

WebSense is a software product that prevents users on a network from accessing web sites based on an site-denial list. The site-denial list is created by selecting predefined categories determined by WebSense employees. WebSense differs from many filtering products by categorizing websites based upon an actual visit by an employee. In addition to the filtering capabilities, WebSense also offers extensive site access reports based on firewall logs.

Currently, the 9th Circuit is the only gateway with both Firewall-1 and WebSense installed and operational. The 5th Circuit is waiting for a new server before installation of WebSense. The AO has both installed, but has not implemented WebSense's blocking feature. They are now awaiting the outcome of your deliberations.

The Eight and Tenth Circuit's were contacted and both elected to leave the blocking software intact pending the results of your review.

Appropriate Usage Policies.

The Policy statement approved by the USJC in September called for each court to establish responsible usage policy statements. The language of that policy is included in Information Resources Management Bulletin (IRM 97-19) put out by the Administrative Office. The full Bulletin is attached. In says in part:

Experience in the private sector and in other government agencies has revealed four principal areas of concern associated with uncontrolled access to the Internet for employees: institutional embarrassment, misperception of authority, lost productivity, and capacity demand. When accessing the Internet from a judiciary gateway, users need to keep in mind several points: they should use discretion and avoid accessing Internet sites which may be inappropriate or reflect badly on the judiciary; those not authorized to speak on behalf of their units or the judiciary should avoid the appearance of doing so; users should exercise judgment in the time spent on the Internet to avoid an unnecessary loss of productivity or inappropriate stress on capacity.

The Ninth Circuit also requires that Internet usage policies be established by each court unit executive before access is given to their users. All of the courts within the Ninth Circuit have provided us with formal procedures with the exception of the Court of Appeals. We have been bringing their users online with the approval of the Clerk of Court. We have not required formal written policies by the unit executives of the Eight and Tenth circuits.

We developed and circulated a "model" usage policy for the consideration of the courts. Most of the Court units within the Ninth Circuit adopted this policy or some variant on it. The model policy follows:

Office of the Circuit Executive Model Policy:
"Policy for the Acceptable Use of the
Public Internet Network"

June 30, 1997

Introduction:

The following model policy for acceptable use of the public Internet network is supplied to court units so they may more easily draft a use policy that reflects local business needs. Prior to any court supplying widespread Internet access to employees via the Judiciary's Data Communications Network, it is strongly suggested that they adopt this policy, or a modified version, and make it available to all staff that will be able to access the Internet.

Policy for the Acceptable Use of the Public Internet Network

General Policy

1. Use of the public Internet network accessed via computer gateways owned, or operated on the behalf of the United States District Court for the District of XXX ("the Court") imposes certain responsibilities and obligations on Court employees and officials ("Users") and is subject to Court policies and local, state and federal laws. Acceptable use always is ethical, reflects honesty, and shows restraint in the consumption of shared computing resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and an individual's right to freedom from harassment and unwarranted annoyance.

2. Use of Internet services provided by the Court may be subject to monitoring for security and/or network management reasons. Users of these services are therefore advised of this potential monitoring and agree to this practice. This monitoring may include the logging of which users access what Internet resources and "sites." Users should further be advised that many external Internet sites also log who accesses their resources, and may make this information available to third parties.

3. By participating in the use of Internet systems provided by the Court, users agree to be subject to and abide by this policy for their use. Willful violation of the principles and provisions of this policy may result in disciplinary action.

Specific Provisions

1. Users will not utilize the Internet network for illegal, unlawful, or unethical purposes or to support or assist such purposes. Examples of this would be the transmission of violent, threatening, defrauding, obscene, or unlawful materials.

2. Users will not utilize Internet network equipment for partisan political purposes or commercial gain.

3. Users will not utilize the Internet systems, e-mail or messaging services to harass, intimidate or otherwise annoy another person.

4. Users will not utilize the Internet network to disrupt other users, services or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses, and sustained high volume network traffic which substantially hinders others in their use of the network.

5. [Local verbiage Option A]

Users will not utilize the Internet network for private, recreational,

non-public purposes.

[Local verbiage Option B]
Use of the public Internet system will be treated similarly to "local telephone calls," and staff will keep the use of the Internet system for personal or non-public purposes to a minimum. Users should exercise discretion in such use, keeping in mind that such use is monitored and traceable to the court and to the individual user.

6. Users will utilize the Internet network to access only files and data that are their own, that are publicly available, or to which they have authorized access.

7. Users will take precautions when receiving files via the Internet to protect Court computer systems from computer viruses. Files received from the Internet should be scanned for viruses using court-approved virus scanning software, as defined by Court policy.

8. Users will refrain from monopolizing systems, overloading networks with excessive data, or otherwise disrupting the network systems for use by others.

Blocking Software.

The Administrative Office has established a policy for their own employees that prohibits any unofficial use of the Internet. They actively track the Internet activity of all of their employees and have fired at least two employees for accessing pornographic material. An AO employee who is on the Internet for official business and inadvertently accesses a pornographic site must file a form explaining the event. According to the AO, many of the executive branch agencies have adopted this same "tracking" approach.

An alternative to tracking is to "block" access to selected sites. There is a variety of software packages that accomplis this. Some of them search the web using keywords and automatically block any site that includes an objectionable word. The WebSense software that was selected by all three national sites uses a different approach. They have employees who review all new sites and classify them.

WebSense serves a dual purpose. It provides the capacity to block sites based upon category and has an add-on product that simplifies report generation from the firewall logs. The categories that WebSense uses are determined by a visit by a WebSense employee. This method is much more effective than other products that use a keyword, or imbedded rating approach.

We are using WebSense to block three categories of sites: pornographic, adult, and

sexuality/lifestyles. We implemented the blocking for several reasons:

1. There is no reason that a user, during the normal course of business, needs access to these sites.
2. Visits by judicial employees to these sites could result in embarrassment to the judiciary. All visits to websites are logged at the firewall for security purposes, but they are also logged at the site that is visited. Marketing agencies often use these figures to determine site popularity and advertising rates. Since every visit to a site by a user from the judiciary results in a **uscourts.gov** name resolution in their log, this can cause potential embarrassment for the judiciary.

3.Potential for sexual harassment claims due to employees "posting" sexually explicit images on their screen while viewing and/or downloading pictures from these sites. (See attached article)

Judge Kozinski's memo alerted us to an issue of which we were previously unaware: gay, lesbian and bisexual sites are restricted by our current category restrictions. WebSense has grouped all gay and lesbian sites into the sexuality/lifestyles category. The "pornographic" category is only for heterosexual sex according to WebSense. Unfortunately, if we allow the sexuality/lifestyles category, we will not only allow gay and lesbian bookstores, but also gay and lesbian sex, bestiality, sado/masochism, fetishes, and more. We have contacted WebSense about this unusual classification.
In the meantime, we have the ability to allow sites that are inappropriately blocked. When a user encounters a blocked site that he or she would like access to, he or she can write or call and ask that the blocking for that site be removed.

Considerations for The Judicial Council.

There are a variety of alternatives for you to consider. At one extreme, we could allow absolute unfettered access to the Internet for all employees. At the other extreme, we could establish a complete circuit-wide prohibition against personal use of the Internet similar to the policy in place for employees of the Administrative Office. There are many alternatives between those extremes. The software is fairly flexible and we are not overly limited by technical considerations.

What follows are five variants for you to consider.

1. **No Tracking/No Blocking**. Allow complete access to all sites on the Internet. If we remove our blocking software at the gateway level, all 10,000 users in the three circuits would have full access to all Internet sites regardless of content. The potential for misuse and embarrassment to the judiciary is high. It should be kept in mind that all Internet traffic would

still be logged. Keeping a log at the firewall is essential for maintaining the security of the DCN. The OCE will not scan the logs and look for inappropriate usage. Additionally it should be noted that all of the commercial sites maintain a log of visitors for their site that can trace the visit back to the actual machine that was used to access the site. A visit to any site from a computer coming through this firewall will leave an electronic trail that concludes with...."uscourts.gov".

I asked the staff to run a list of the sites that were visited in the month before we put the blocking software in place. As you can see from this partial listing, there is ample opportunity for institutional embarrassment.

2. **Local Blocking.** Allow complete access through the gateway, but require courts to purchase their own "mini-firewall" to control users access. CAC District court has implemented one of these products, BorderManager from Novell, for this purpose. The advantage of this option is that it is highly flexible and each court unit could tailor their own policies. Unfortunately, this is very costly software. WebSense costs between $2,500 and $10,000 per location plus an on-going maintenance amount. Each location is defined as each place with an independent computer network. In this circuit alone we would be required to purchase and maintain around 50 or 60 copies of the software. This would be an expensive and complex undertaking that would diminish the security and integrity of the Data Communications Network. It would cost a minimum of $125,000 to implement this solution in just the Ninth Circuit.

3. **Full Access to Some Users**. The blocking software that we are using would allow us to offer complete access to a few users based on IP address or network segment. In other words, we could provide Judge Kozinski's chambers with complete access and continue to block others. This solution is possible if there are only a handful of sites that are given this level of access. If there were more than a very few of these types of exceptions, it would quickly overwhelm our staff and the other over local systems staff.

4. **District Wide Access.** A viable option is to allow each district and the Court of Appeals to make their own determination as to whether they want to block access to these sites or not. While it is technically possible to allow tailored access to units smaller than the entire district, it would be an administrative nightmare to try and manage such a system. In the Ninth Circuit alone there are 15 districts plus the Court of Appeals. Between the Eight, Ninth and Tenth circuits there are 33 districts and Three Courts of Appeal. If we were to tailor access at the unit level, we would be maintaining sixty unique polices in the Ninth Circuit and up to 125 or so between the three circuits. Exercising this option at anything less than a district wide level is not feasible with current staff due to the extreme administrative workload. The only way to successfully implement this policy would be to receive funding from the AO for a dedicated position.

5. **Current Implementation.** A final alternative would be to continue blocking access to pornographic materials for all users as we currently do. In other words we would leave the

blocking software in tact. If we were to pursue this approach, it would make sense to approach WebSense to see if they could sever the relationship between the gay and lesbian sites and the pornographic sites. This is the safest, cheapest alternative.

STAFF RECOMMENDATION

I recommend that you adopt the following policy governing access to the Internet for all court units within the Ninth:

1. Continue to block access to pornographic sites at the firewall as the default setting.

2. Allow each district (not court unit) and the Court of Appeals to request that the blocking be turned off for the users under their control.

The advantages of this hybrid approach are several:

Each district could elect to have access blocked at the firewall or to offered unlimited access to their users.

Each district could elect to purchase and maintain their own software, but wouldn't be required to.

This system would be fairly easy to maintain at the circuit level since all decisions would have to be made at the district-wide level. All of the court units within a district would have the same policy at the firewall level, either blocking on or blocking off.

OFFICE OF THE CIRCUIT EXECUTIVE

UNITED STATES COURTS FOR THE NINTH CIRCUIT

95 SEVENTH STREET
POST OFFICE BOX 193939
SAN FRANCISCO, CA 94119-3939

GREGORY B. WALTERS, CIRCUIT EXECUTIVE
PHONE: (415) 556-6100
FAX: (415) 556-6179

TO: Hon. Proctor Hug, *Chief Judge*
Greg Walters, *Circuit Executive*

FROM: Matthew Long, *Assistant Circuit Executive for Automation and Technology*

DATE: April 28, 1998

RE: Adult Site Access by Judicial Employees

We have finished processing the firewall logs for the month of February. The actual dates of the logs analyzed are from February 4 to March 3, 1998. This twenty-eight day period gives us a sampling of Internet usage by users from the 8th, 9th, and 10th circuits in the month prior to the installation of WebSense.

We used two methods to try to extract adult site accesses through our firewall. First we used a keyword search on adult-oriented themes to locate domain names that corresponded to sex sites, e.g. sex, porn, adult, etc. Once we compiled a large list of names, we traced the viewing habits of individual users who had visited these sites. This allowed us to augment our database and produce more accurate numbers.

Of the 28,000 different sites accessed in February, approximately one-third did not resolve to a name, thus making it difficult to get exact figures for adult site accesses. For example, a site would be listed in the log as 207.204.211.25 instead of www.sex.com. Many adult sites deliberately do not resolve, either to save money on name registration or to maintain anonymity. I believe our figures to be a good estimate, but could be as much as 10-25% below the actual numbers.

Here are the rounded figures for Internet access through our gateway:

Total web accesses*:	2,500,000
Total sites accessed:	28,000
Total adult site accesses:	**90,000**
Total adult sites accessed:	1,100
Adult site access percentage:	3.6%
Adult site percentage:	3.9%

*Every time a user clicks on a link on a webpage, it counts as a web access hit. For

example, if a user visited www.usatoday.com clicked on a story link and then clicked the back button, our log would show three web accesses and one site accessed (usatoday).

I've attached a partial listing of some of the adult sites accessed through our firewall. The list contains some very graphic names, but should be a good sample of the types of sites that were accessed. We have not verified that all of these are adult sites; therefore, there may be several on the list that are not. The full 28-page listing is available if you need it for the council meeting.

Attach.

Adult Sites Accessed through the Ninth Circuit Gateway

February 4 to March 3, 1998

Partial Listing

1adultvideo.com
1porn.com
69oralsex.com
adamsxxx.com
adult7.com
adultad.com
adultcentral.com
adulthosting.com
algol.cybererotica.com
allteens.com
amateurfresh.com
amateurindex.com
amazon-cum.com
asiannudes.com
assland.com
babe.swedish-erotica.com
babes.sci.kun.nl
bestgirl.com
bigchicks.com
bitemypussy.com
blondes.nudepictures.com
butts-n-sluts.com
cam.digitalerotica.com
canadianschoolgirls.com
comfortablynude.com
ctc.sexcenterfolds.com
cubby.shaven-girls.com
cumberland.premiernet.net
cyber.playboy.com
cyberteens.www.conxion.com
electraporn.com
erotic-x.com
eroticnet.babenet.com
famousbabes.com
faraway.cybererotica.com
fetishtime.com
foot-fetish.com
freehardcorelive.com
gay.adultclubs.com
gayteenboys.com
girls2die4.com

girlsinlingerie.com
girltown.com
girltown.tierranet.com
gorgeousgirls.com
hardcore.sexmonkey.com
hardcoresex.com
hot-live-sex.com
hotcunt.hotcunt.com
hotporno.com
hotsexlinks.com
hotteen.com
hotteensex.com
karasxxx.com
kristysteenpalace.com
kristysteens.com
lynx2.sexbooth.com
mail.amateurdirectory.com
mail.cum2oasis.com
mail.freebie-sex.com
naked4u.com
nude-celebs.com
nudeadultpics.com
nudeceleboutpost.com
nudeeroticsex.com
nudehollywood.com
nudes.com
one.123adult.com
orientalpussy.com
pg.pornoground.com
phils-porno-parlor.com
pics.callgirls-xxx.com
porndirectory.com
porndog.mco.net
pornrock.com
pussybabe.com
pussyland.com
pussyteens.com
realhardcore.com
s2.nastyfetish.com
sexdragon.com
sexpictures.com
sexploitation.com
sexscape.com
sexsluts.com
sexwars.com

sexworlds.com
showgirl.net
sinfulteens.com
sixchicks.com
sluttyamateurs.com
sucksex.com
supermodels.nudepictures.com
superpics.adulthosting.com
technoteen.com
teenbutts.com
teensexworld.com
teensexx.com
teentwat.teentwat.com
teenvirgins.com
time4sex.com
traxxx1.focus.de
ultrafreexxx.com
ultrahardcore.com
universaladultpass.com
vh1.adultlinks.com
vividsex.com
vlad.adultorigin.com
vlad2.absolutexxx.com
voiceofwomen.com
w3.purehardcore.com
west.sucksex.com
wetfetish.com
ww1.voyeurweb.com
www.2adult.com
www.3sex.com
www.4adultsonly.com
www.aahsex.com
www.adult2.com
www.adultbytes.com
www.adultlink.com
www.adultphotos.com
www.adults-online.com
www.adultsights.com
www.adultswap.com
www.advancingwomen.com
www.all-americangirl.com
www.allerotica.com
www.altsex.org
www.amateur-x-pics.com
www.amateur-x.com

www.amateurexhibitionists.com
www.amateurmagazine.com
www.amateursonline.com
www.amateursonly.com
www.amateursweb.com
www.analbabes.com
www.asexycafe.com
www.asian-teens.com
www.asianxxxpics.com
www.atomicpussy.com
www.awsomebabes.com
www.axxxess.com
www.babes4free.com
www.bigsextoys.com
www.bisexualbabes.com
www.celebritybabes.com
www.chatgirls.com
www.clubsex.net
www.cockorama.com
www.cocktailbar.com
www.collegenudes.com
www.cruisingforsex.com
www.cumasyouare.com
www.cumorahcu.com
www.cumpany.com
www.cyberporn.inter.net
www.cyberporndirectory.com
www.dailyxxx.com
www.delicious-pussy.com
www.dormgirls.com
www.dreamgirls.com
www.erotica.co.uk
www.eroticpix.inter.net
www.eroticworld.net
www.euroflixxx.com
www.fastporn.com
www.finegirls.com
www.free-xxx-pictures.com
www.free-xxx-porn.com
www.free-xxxpics.com
www.freegirlsex.com
www.gayhardcore.com
www.girl.co.jp
www.girlies.cz
www.girlsagent.com

www.girlswithgirls.com
www.groupsexdogs.com
www.hardcoreclub.com
www.hollywoodnudes.com
www.hollywoodteens.com
www.hot4sex.com
www.hottestwomen.com
www.hotwiredxxx.com
www.hotxxxteens.com
www.imengonude.com
www.internet-xxxmodels.com
www.intersex.inter.net
www.jessicasteen.com
www.lasvegassex.com
www.lensexpress.com
www.leo-xxx.com
www.littleteen.com
www.maturebabes.com
www.naked-celebs.com
www.nastychat.com
www.nastysex.com
www.net-erotica.com
www.net2sex.com
www.onlyxxx.com
www.playgirlmag.com
www.playsex.com
www.porn-king.com
www.pornado.com
www.porndorm.com
www.pornet.com
www.pornexchange.com
www.pornocopia.net
www.pornojapan.com
www.pornotimes.com
www.pornplus.com
www.pornstories.com
www.pornusa.com
www.powerotic.com
www.private.sex.se
www.purehardcore.com
www.pussylink.com
www.pussyvision.com
www.realamateur.com
www.realsex.com
www.ripvoyeur.com.hk

www.schoolgirlz.com
www.sex-crawler.com
www.sex.se
www.sex4ya.com
www.sexcabin.com
www.sexcat.com
www.sexclubxxx.com
www.sexdv8.com
www.sexe.com
www.sexelsewhere.com
www.sexfiction.com
www.sexfinder.com
www.sexfreebies.com
www.sexgalleries.com
www.sexgalore.com
www.sexhigh.com
www.sexhungryjoes.com
www.sexinabox.com
www.sexinc.com
www.sexlink.net
www.sexodus.com
www.sexplanet.com
www.sexshopper.com
www.sexsounds.com
www.sexsource.com
www.sexswap.com
www.sextv.com
www.sexvote.com
www.sexybloomers.com
www.sexyfriends.com
www.sexyinternet.com
www.sexypics.com
www.sexysin.com
www.sexysites.com
www.showgirl.com
www.smokingpussy.com
www.smutcity.com
www.smutland.com
www.smutpix.inter.net
www.sororitypussy.com
www.spice-girls.co.uk
www.tecumseh.com
www.teen-porn-club.com
www.teenage-tarts.com
www.teenchallenge.com

www.teenhideout.com
www.teenie-sex.com
www.teennympho.com
www.teenpanties.inter.net
www.teens-n-colors.com
www.teenstar.com
www.teenstories.com
www.teeny.com
www.thesluts.com
www.totallysex.com
www.uk.playboy.com
www.ukhardcore.com
www.ultimatehardcore.com
www.voyeurplay.inter.net
www.voyeurstories.com
www.voyeurweb.com
www.xtremehardcore.com
www.xxx-18.com
www.xxx4u.net
www.xxxcat.com
www.xxxcounter.com
www.xxxman.com
www.xxxreferral.com
www.xxxstories.com
www.xxxstuff.com
www.xxxvisions.com
www.youngerotica.com
www.zoosex.com
www1.playboy.com
www2.adultsights.com
www2.amateurfresh.com
www2.playboy.com
www4.playboy.com
www7.hollywoodhardcore.com
www8.girlsofrussia.com
wwwserv.weirdsex.com
xxx-pics.net
xxx.com
xxxads.adulthosting.com
xxxempire.com
xxxlinkexchange.com
xxxnewspics.com
xxxo.com
xxxvids.com
xxxxxx.com

EXHIBIT 2

October 12, 2007

Judge Ralph K. Winter Jr., Chairman
Judicial Conference Committee on Judicial Conduct and Disability
US Court House, 141 Church Street
New Haven, CT 06510

Dear Judge Winter,

RE: Public Comment on Proposed Rules Governing Judicial Conduct and Disability Proceedings.

TEST CASE TO ASSESS, IN PART, THE ADEQUACY OF THE PROPOSED RULES

The following factual case is offered as a possible test of the adequacy of the proposed new rules. Although the Breyer Committee discussed in general several instances when Circuit Councils did not deal appropriately or adequately with complaints filed against a few Federal Judges, it is not clear if the Committee considered this case. When given the facts which were publicly known, lawyers at the General Services Administration (GSA) and the Administrative Office of the United Stated Courts (AO) and even Chief Justice William H. Rehnquist agreed that at least one felony probably had been committed by a United States Circuit Judge acting in concert with a Circuit Executive. The facts were known by the Circuit Chief Judge, the Circuit Council and indeed by the Judicial Conference of the United States. Yet, no complaint was filed against the Judge by the Circuit Chief Judge or by any member of the Circuit Council or the Judicial Conference. Moreover, although probably outside the purview of your Committee, to my knowledge, no disciplinary action was taken against the Circuit Executive by the Circuit Chief Judge or the Circuit Council, which clearly did have jurisdiction.

It is my strongly held view that this total absence of action is the worst example of failure by those responsible for disciplining Judges that I witnessed during my 21 years as AO Director.

I present this case so that your Committee can determine if disciplinary action was mandated against the offending Judge under the old Rules and Statutes. If not, do the new Rules close what is thus a gaping loophole in the old Rules and mandate disciplinary action, and by whom?

Commendation for Winter and Breyer Committees

First let me commend you and your committee for the draft rules that you have proposed to amend current Judicial Conduct and Disability Rules. My admiration extends also to the report to the Chief Justice by the Judicial Conduct and Disability Act Study Committee entitled "Implementation of the Judicial Conduct and Disability Act of 1980," Chaired by Justice Stephen Breyer with 5 Federal Judges also serving. Taken together, these two reports will do much to maintain and increase public and Congressional confidence in the Federal Judges as your new Rules are applied by the Circuit Councils in considering complaints of misconduct filed against Federal Judges.

As you know, over the years some leaders in Congress and Academe have suggested that in some instances the Judges on Circuit Councils have not been willing to discipline appropriately their colleagues when complaints were filed. Moreover, some Circuit Chief Judges have failed to file complaints against their colleagues even though the facts apparently justified such action.

As you know, I served as Director of the Administrative Office of the United States Courts (AO) for 21 years. Early in my service Representative Robert Kastenmeyer (D. Wisc.) Chaired the House Judiciary Committee. He believed that Circuit Councils may not have been carrying out their duties in some instances when complaints were filed against Federal Judges House hearings were held and although the Judiciary was urged to improve, no legislative action was taken at that time. Then about three years prior to my 2006 retirement, major concerns were expressed by several current Congressional members alleging lack of objectivity by Circuit Councils in handling some complaints particularly by Representative James Sensenbrenner (R. Wisc.) then

Chairman of the House Judiciary Committee. Allegations were made that there was an "old boy network" of Judges who protected and would not act against their colleagues. He was sharply critical of what he perceived to be the failure of certain Circuit Councils to deal appropriately or adequately with complaints against a few Judges. He expressed these views with a high degree of passion both publicly and in two personal appearances before the Judicial Conference of the United States. Of course I had kept Chief Justice William Rehnquist informed of his criticisms well before he presided over the Conference services meeting where Sensenbrenner spoke. Then I met with the Chief Justice after the second Sensenbrenner "lecture" and we agreed that he should visit Sensenbrenner at his House office, a most unusual thing for any Chief Justice to do. But the Chief agreed that this issue was sufficiently important to do so. After talking with Sensenbrenner he told him that he planned to appoint a special committee of Judges to study the issue, to be chaired by Justice Stephen Breyer.

At least two very important results came from that process; first, the Judiciary bought some time because had there been no such actions, Chairman Sensenbrenner made it very clear that he was going to impose an Inspector General on the Judiciary to make sure that the Judges behaved themselves. Second, it has now resulted in the excellent work product from both the Breyer committee and your important Conference committee. If adopted, your proposed Rules will increase the confidence in Judges among Congress, the public, the Bar and the Media.

My comment on the proposed Rules themselves will be confined to posing a factual situation, which in my view should have been considered by the Ninth Circuit Council but never was. In my opinion it is still a dark cloud hanging over the reputation of the Judicial Branch. The current rules could and should have been applied through a formal complaint against the Judge involved either by the Chief Circuit Judge or other Judges. I believe the current rules allow and may require a complaint by the Chief Judge of the Circuit. However such a complaint never was forthcoming from her or from any other Judge.

Factual Case to Test the Proposed New Rules

In 2001, Ninth Circuit Judge Alex Kozinski, in the company of the then Circuit Executive Greg Walters and perhaps one other Ninth Circuit Judge illegally (according to GSA's lawyers and ours) seized and then sabotaged the vital Judiciary Internet Gateway Security System then located in San Francisco. As a result thousands of computer hackers throughout the world were permitted to invade the records of courts, judges and court staff not only in the Ninth Circuit but also in the Eighth and Tenth Circuit, which were similarly served by that Gateway. Moreover, skilled hackers once they broke through the system in San Francisco could penetrate into every Court in the United States. The National Security Agency (NSA) expert who consulted with the Judicial Conference Internet and Technology (IT) Committee said that from a security standpoint this action by Kozinski was "insane."

GSA lawyers who are responsible for computer systems policy in the Federal government said that this action was not only "illegal" but constituted at least one felony. They along with our own internal lawyers cited title 18 USC1361, which states that:

> "whoever willfully injures or commits any depredation against any property of the United States, or of any Department or Agency thereof ... shall be punished by a fine of $1,000 and depending on the circumstances a prison term of 1 to 10 years."

Likewise section 1362 states that:

> "whoever willfully injures or maliciously destroys any ... system, or other means of communications, operated or controlled by the United States ... or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system or attempts or conspires to do such an act, shall be fined under this title or imprisoned not more than 10 years or both."

For your Committee to determine the application to this case of either the old or your proposed new rules, it is important to know the facts that led up to this extraordinary unsupportable action by Judge Kozinski and Greg Walters. During 2000 and 2001 there was a major increase in the use of Internet Bandwidth by Federal Courts throughout most of the United States. This greatly elevated the cost and gave rise to the strong suspicion that the court computer systems were being abused. This was of great concern to the Judicial Conference Information Technology (IT) Committee, which had been given considerable responsibility by the Judicial Conference to monitor the costs and management of judicial computer systems throughout the country. The Committee, then Chaired by the late District Judge Ed Nelson, directed my staff at the AO to monitor internet bandwidth use throughout the country to determine why there had been such a major increase in bandwidth use. The Committee also directed that the study must be confined solely to general bandwidth information. The staff was expressly forbidden to examine either e-mail or individual computers used by any Judge or court employees anywhere in the country. This was done to assure privacy.

When this initial bandwidth study was completed, the results were presented to the IT Committee which learned that by far the greatest proportion of the bandwidth increase occurred through the illegal downloading of pornography and some other movies and NAPSTER music on court computers in Federal courts on Federal time throughout the United States. In short there was a wholesale violation of the Federal law and waste of taxpayer funds throughout the country, particularly in 39 courts.

Judges and Court Employee Privacy Fully Protected

It is important to note once again that my staff faithfully followed the direction of the IT Committee and confined their study solely to internet bandwidth use. Thus the computers and e-mail of individual court employees, law clerks and Judges were not examined or studied. The IT Committee then issued instructions which in most instances, I was asked to send to the entire court family so that this systematic breaking of

Federal Law in the Courts would be ended, and the Judiciary avoid serious embarrassment. But Judge Kozinski chose to comment publicly to the New York Times, to at least one National news magazine and wrote a lengthy essay for the Wall Street Journal editorial page on his mistaken version of the study. By doing so, he created considerable media attention and public awareness to the Judiciary's severe problem of illegally using court computers.

The facts described above are indisputable since Judge Kozinski publicly admitted his role in illegally seizing the vital Internet security facility disabling it, and thus opening judicial records up to thousands of computer hackers throughout the world endangering the security of the entire Judicial Branch. Not only did he admit his illegal actions but he also boasted about them in the National press. One National magazine published his picture with an article in which he recounted his sabotage of the security system featuring his comment "What is a Judge to do?" Virtually every other Judge in the United States would have said that what a Judge is to do is obey Federal law, not waste Federal money and not to believe apparently that a Federal Judge is above the law just because of his office. Judge Kozinski was so proud of his sabotage action that he actually filmed a reenactment and made copies of the tape, one of which was sent and viewed at a nationwide Judiciary computer staff meeting in Jacksonville, Florida. On the tape he described triumphantly to all the many court computer experts assembled from throughout the country precisely how he seized the computer security facility and disabled it so it would no longer protect Judge's records. Present, however, was the great Chairman of the Judicial Conference IT Committee which had directed that the bandwidth use study be made. Judge Nelson recognized that the Kozinski tape was intended in part to be a direct attack on him and his committee before the professional staff in order to embarrass him and his fellow committee members. He said he could not understand how Judge Kozinski could possibly justify his illegal action to destroy the security system and endanger Judges records and then reenact the crime on film.

For Judge Nelson and for any objective observer it was impossible to connect the destruction by Kozinski of the security system with a Committee request to study bandwidth which in no way violated the privacy of Judges or court staff but did reveal that some employees in

Federal Courts, at least 39 Courts, were downloading pornography and some even viewing them in the court facilities on court time. Judge Nelson believed that the Kozinski action was designed entirely to cover up this outrageous waste of Federal taxpayer money and equipment in too many of the courts.
Kozinski even volunteered publicly that one of his law clerks had downloaded pornography in his court. He did not mention the extent to which he and his other law clerks also downloaded pornographic movies and NAPSTER music.

Chief Justice Rehnquist was appalled by the Kozinski Security Sabotage

When Chief Justice William Rehnquist learned of Kozinski's actions and then learned that he was boasting in public about his deliberate violation of Federal law he said "Tell Alex to watch pornography at home and not download and watch it in the courts."

Chief Justice Rehnquist was so disturbed by Kozinski's actions and his public boasting that he directed the Judicial Conference Executive Committee immediately "to take firm disciplinary action against all those involved" including, of course, Kozinski and Walters. He also believed that the Kozinski/Walters action might have been taken with the tacit or active endorsement of the Chairman of the Circuit Council, Judge Mary Schroeder, and perhaps the entire Ninth Circuit Council. Thus the minutes for the Executive Committee emergency teleconference of May 31, 2001 show that the Chief Justice "concluded something needs to be done that would get the attention of the Ninth Circuit Council." He said that "more needed to be done than a remonstrance and more than a slap on the wrist." He directed the Committee and me to determine if the Ninth Circuit Council Judges and Circuit staff could be cut off completely from the data communications network (DCN) thus depriving them of their computers and other automated facilities. Indeed he specifically asked us, "Can we cut off computers?"

At the time of the Executive Committee meeting, Associate AO Director Pete Lee was in Alaska attending a gathering of Chief Judges from the Ninth Circuit Chaired by Circuit Chief Judge Mary Schroeder. He

reported on the phone for the Executive Committee and me that she was "now talking to them" (the Chief Judges) and said "she is afraid that the record of the extensive downloading of pornography in the courts will be embarrassing to some of the Judges who are up for Supreme Court or other appointments." According to Lee, she also said that she and a Circuit Executive, Walters, were willing to "put the security system back up" and make it operational "if we (the Executive Committee members and the AO) agree not to measure sex explicit movies that are being down loaded in the courts." Significantly, there was no talk at the Alaska meeting according to Lee about fear of reading Judges e-mail which they knew did not occur. Rather the concern was about possible embarrassment to Judges caused by reports of pornography downloading in the Courts.

No Disciplinary Action Taken

Given the gravity of this situation, coupled with the exceptionally strong views of the Chief Justice, I was truly surprised when a narrow majority of the Executive Committee refused to recommend or take any disciplinary action with respect to Kozinski or Walters or the Ninth Circuit Council. All they agreed to do was to have the Chairman, District Judge Charles Haden (N.D. West VA) call Chief Judge Schroeder to work out an agreement to restore that the security system to working condition. Haden then promised to her that the IT committee would no longer require the monitoring of bandwidth use by the courts. In short, Judges Schroeder and Kozinski and Circuit Executive Greg Walters got precisely what they wanted. There would be no discipline of the offenders. Moreover, no longer would there be any monitoring of the extent to which pornographic movies and NAPSTER music were being illegally downloaded by Federal Courts. Later, the Judicial Conference took what can only be described as cosmetic action essentially leaving it up to each individual court to develop a system of its own in the hope that Federal law is not being violated in that court. The Administrative Office was directed by the Conference to obtain an annual report on the quality and adequacy of the plans developed by each court throughout the country to require legal compliance. Based upon the last report which I say which was for 1995-96 some courts have no plan at all while other courts have

inadequate plans. Fortunately, some have good working plans. In short, even the cosmetic action goals are not being met in too many of the courts throughout the country. If this sorry state of affairs is once again treated in the media and considered by Congress, the Judiciary stands to be held up to ridicule and embarrassment throughout the United States.

Result of the Failure to Discipline

The conclusion reached in this case study is that a Judge and/or a court administrator can violate Federal law and commit felonies but will not be disciplined in any way. Likewise, in too many courts, Judges and court staff appear largely to be free to download pornography and NAPSTER music if they choose without detection and with no discipline built into the system of these courts to assure that Federal law is being obeyed.

Chief Justice orders Removal of an Internet Security Gateway from the Ninth Circuit

To say that Chief Justice Rhenquist was angry about the failure of the Conference Executive Committee to carry out his direction to discipline the Ninth Circuit perpetrators coupled with the limited cosmetic action taken by the Judicial Conference along with the failure of the Ninth Circuit to consider complaints would be a gross understatement. The Chief Justice lectured the Executive Committee sternly about their failure to take appropriate action to discipline Judge Kozinski, Greg Walters and the Ninth Circuit Council.

As stated, Chief Justice Rehnquist was highly disturbed about what he perceived to be the complete failure of the Ninth Circuit Council and Chief Judge Schroeder either to take disciplinary action against Judge Kozinski and/or on Circuit Executive Greg Walters. However there was one action that he could take to further express his displeasure and restore some integrity to the system. He ordered me to remove the Internet Gateway security system from San Francisco taking it entirely out of the Ninth Circuit and relocating it in another Circuit. He did this so that neither Judge Kozinski nor Greg Walters nor the Circuit Council could

again sabotage Judicial Branch security equipment and thus endanger the security of the entire Federal Court system. It is now located near Kansas City, Missouri.

Chief Justice Rehnquist further evidenced his continuing acute displeasure caused by the failure of the Ninth Circuit Council or the Executive Committee to take "stern disciplinary action. When Judge Schroeder recommended appointment to the Conference IT Committee of the other Circuit Judge who reputedly accompanied Judge Kozinski, he turned it down flatly. Instead he appointed a District Judge from Idaho whom I recommended.

Judicial Conference Procedures Ignored by Kozinski

Sabotaging the security system was not the only avenue available to Judge Kozinski if he objected to the policy of the Judicial Conference IT Committee seeking to uncover and forestall possible waste, abuse, and violation of Federal law through examining bandwidth use throughout the Judicial Branch. The IT Committee is a creature of the Judicial Conference and responsible to it. Kozinski could have complained to Chief Judge Schroeder who is a member of the Conference by right of office and to the elected District Judge on the Conference from the Ninth Circuit and to ask for a reconsideration of this policy and if necessary ask that it be done on an emergency basis. He also could have lodged a complaint and request for similar action with the Chief Justice who presides over the Judicial Conference and appoints all Conference Committee members including the IT Committee. Likewise he could have gone to Judge Ed Nelson the Chairman of the IT Committee and to the Committee itself seeking such action. The Ninth Circuit has always had a representative Judge who serves on that Committee but there is no record that Kozinski ever complained to that Judge. Thus, instead of going through the accepted Conference channels, which permit expeditious action when necessary, he chose to take the law into his own hands and constitute himself a judicial vigilante. He decided to defy openly both the Conference Committee and the Conference itself presided over by the Chief Justice and preceded to violate Federal Criminal law, which clearly applies to him. Moreover he and Greg Walters violated the

contract made between the Ninth Circuit Executive and the IT Committee in which the Circuit staff agreed to manage the internet security gateway in San Francisco in behalf not only the Ninth Circuit but also the Eighth and Tenth Circuits. Incidentally neither Judge Kozinski nor Judge Schroeder nor Greg Walters consulted with either of the other two Circuits before summarily shutting down the system thus endangering all Judges and court staff in both of those Circuits.

Kozinski "Privacy" Straw Man

Judge Kozinski obviously decided that he could not prevail in the public relations arena if he tried to justify illegally sabotaging the Judiciary's Internet security system in San Francisco solely in order to assure that Judges and court staff could continue to illegally download pornography and NAPSTER music. Therefore, he created a fictitious straw man in an attempt to explain his extraordinary unilateral vigilante action. He falsely claimed both inside the Judiciary and extensively throughout the public media that the bandwidth survey mandated by the IT Committee somehow resulted in Judge's e-mail being read and their individual computers monitored. He did this even though Judge Nelson told him that it wasn't true! No Judge's e-mail was read or monitored in any way nor were their computers monitored. Unfortunately, Kozinski managed to persuade some uninformed media and indeed some of his fellow Judges who did not know the facts that he was the great defender of their privacy. In fact, he was the defender solely of the unfettered ability of all Judges and court employees to illegally download pornography and view it in Federal courts, an objective with which no Federal Judge or Congress would agree.

To my knowledge, the only time individual computers ever were examined to determine if they were being used for illegal purposes was carried out by the Ninth Circuit Council itself in 1998, not by the IT Committee or the AO. The Council discovered that there was a significant amount of abuse in the Ninth Circuit. But there is no record that the Circuit Council disciplined the offenders however.

COMMENT AND QUESTIONS ON THE APPLICATION OF THE PROPOSED NEW RULES TO THE ABOVE FACTUAL SITUATION

1. The conduct described above was not known to members of the Bar or to litigants. It appears therefore from the Committee commentary on Rule 3 that there are only two ways a "complaint" could be filed against Judge Kozinski. One would be by a knowledgeable Federal Judge. The second is that the "complaint" may be "identified" by the Chief Judge. But in the absence of a complaint by another Judge, is the Chief Circuit Judge required to file a complaint? For example, in the above-described situation Chief Judge Schroeder was fully aware of what Judge Kozinski had done but neither she nor any informed Judge filed a complaint. The comment under Rule 3 seems to say that the Chief Judge is not required to file a complaint but "may" file and "often is expected to trigger the process" by "identifying a complaint". Is this a case when a complaint was "expected" to be filed or where one "must" be filed by the Chief Judge?

In the test case, it is theoretically possible that a Ninth Circuit staff member or someone from the AO who were aware of these facts, as indeed many were, could file a complaint against Judge Kozinski. However as a practical matter this likely would not work because of the probable repercussions against such employees. Thus, if the Circuit Chief who, is aware of such misconduct does not elect to identify a complaint, this creates an important loophole in the regulations, which would allow such illegal conduct to go unchallenged. The proposed rules of the Committee ought to consider the possibility of making such action mandatory for the Circuit Chief Judge.

2. If the Circuit Chief Judge is not only aware of possible misconduct or illegal action by another Judge in the Chief's Circuit and may have actually approved or ratified the misconduct or illegality in advance, it is virtually certain that the Chief Judge would not file a complaint. The new Rules as you have proposed them do not appear to deal with this very real possibility. You may wish to

revise the rules to set up an alternate procedure to make sure that a complaint is filed in such circumstances.

3. It does not appear from the existing Rules or the proposed new Rules that there is a statute of limitations that applies to the filing of a complaint of misconduct against a Federal Judge. If that is the case and if the statute has not run, a complaint could still be filed against Judge Kozinski for the illegal action that he took in 2001. Is the Chief Judge required to file a complaint now under the old rules?

4. Under the new Rules, if Rule 5(a) governs and the requirements of Rule 7 and Rule 3(a) too have been met and no complaint has been filed under Rule 6, a Chief Judge "must identify a complaint" and by written orders stating the reasons, begin the review provided in Rule 11. In your Committee's view, is Judge Schroeder obliged to file such a complaint? If so, this probably means that she may be obliged to file one.

5. Rule 29 of your proposed rules provides that the new rules "will become effective 30 days after promulgation by the Judicial Conference of the United States." Thus Judge Schroeder would have to file a complaint, under the new rules but they may not be in effect by November 8, 2007 when she must step down as Chief Judge. If she refuses, who must file a complaint prior to November 8th if anyone?

6. Under current law Judge Alex Kozinski will become the new Circuit Chief Judge on November 8, 2007 succeeding Judge Mary Schroeder. If approved, the new rules will be in effect after Judge Kozinski becomes the Chief Judge. At the time is Chief Judge Kozinski obliged to issue a complaint against himself? I assume the answer is no. I further assume, however, that he would be disqualified under Rule 25. Therefore the new Rules require that the complaint "must be assigned to the Circuit Judge in regular active service who is the most senior in date of commission of those who are not disqualified." If most or all of the members of the current Circuit Council were members of the Council when

Judge Kozinski took his illegal action in 2001, then I assume that the Rules may require each of those individuals to be disqualified particularly if in 2001 they approved Kozinski's illegal action in advance. However Rule 25(G) provides that notwithstanding any other provision of these rules to the contrary, a member of the Judicial Council who is a subject of the complaint may participate in the disposition thereof if the Judicial Council votes that it is necessary and appropriate and in the interest of sound Judicial administration that such subject Judges should be eligible to act. Does this open the door for Judge Kozinski to participate in the Committee handling of his complaint or one filed against him even though he is disqualified as Chief Circuit Judge because he would be the object of the complaint? That section does appear to open the door to him to participate and for any other members of the Council who in 2001 approved his actions in advance, if that occurred.

7. It is clear that the proposed Rules apply only to Federal Judges. They do not therefore cover a Circuit Executive such as Greg Walters who aided and abetted in the committing of a felony according to the facts and the analysis of various lawyers. There is no record that the Circuit Chief Judge or anyone else disciplined him. This clearly is an embarrassment to the Judicial Branch particularly since Walters currently is working on 'detail' for the Administrative Office, which is supervised and directed by the Judicial Conference whose policies and rules he openly defied. This is a notable loophole and your committee may wish to direct an inquiry to the appropriate Judicial Conference Committee, probably Judicial Resources, suggesting that this loophole should be repaired.

In summation: As a result of the illegal action taken by Judge Kozinski, Greg Walters and perhaps one other Ninth Circuit Judge, coupled with the total failure of the Ninth Circuit Council and the Judicial Conference even to consider disciplining for Judge Kozinski under current law and Rules procedures, the Federal Judiciary could be censured by Congress for permitting its laws to be openly flaunted with no response by the Judiciary. Also, it could be justifiably

criticized by the media. This is particularly true and doubly serious because the disabling of the security system obviously took place for one reason and one reason only namely that Judge Kozinski and his allies wanted to make it possible for Federal Judges and court staff to be totally free of detection when or if they download illegal pornography movies and NAPSTER music on Federal Court computers, on Federal Court time, in Federal Court buildings using Federal taxpayer money. Therefore in the interest both of good government and the reputation of the Judicial Branch the new Rules should require Circuit Chiefs and Circuit Councils or suitable alternative Judicial Branch organizations to initiate and consider complaints in this and similar factual situations. Certainly Chief Justice Rehnquist strongly believed that the system must require "stern discipline" in such a situation, discipline that is totally absent thus far and I agree with him fully.

Summary of Central Questions for Your Committee

- Is it mandatory for the Chief Circuit Judge or any other Judge to file a complaint against Judge Kozinski under the old Rules? If not, does your Committee have authority to mandate the filing and consideration of such a complaint?
- Do the proposed Rules require the Ninth Circuit Chief Judge to initiate a complaint against Kozinski that is then considered by the Circuit Council? If not, is it mandatory upon any other Judicial organization such as your Committee to initiate a complaint? If not, your Committee may wish to revise the Proposed Rules to assure that such disciplinary action is taken to restore integrity to the Rules process while at the same time avoiding serious embarrassment to the Judicial Branch for its failure to act.

CC: William R. Burchill Jr., Associate Director and General Council

Mr. William R. Burchill Jr., Associate Director and General Council
Administrative Office of the US Courts
Thurgood Marshall Federal Judiciary Building
Washington DC 20544

Judge Ralph K. Winter Jr., Chairman
Judicial Conference Committee on Judicial Conduct and Disability
US Court House, 141 Church Street
New Haven, CT 06510

EXHIBIT 3

WSJ.com OpinionJournal
from THE WALL STREET JOURNAL Editorial Page

AT LAW

Privacy on Trial

Big Brother is watching you, your honor.

BY ALEX KOZINSKI
Tuesday, September 4, 2001 12:01 a.m.

An open letter to federal judges:

The U.S. Bureau of Prisons maintains the following sign next to all telephones used by inmates:

"The Bureau of Prisons reserves the authority to monitor conversations on the telephone. Your use of institutional telephones constitutes consent to this monitoring. . . ."

I'm planning to put signs like these next to the telephones, computers, fax machines and other equipment used in my chambers because, according to a policy that is up for a vote by the U.S. Judicial Conference, we may soon start treating the 30,000 employees of the judiciary pretty much the way we treat prison inmates.

Exaggeration? Not in the least. According to the proposed policy, all judiciary employees--including judges and their personal staff--must waive all privacy in communications made using "office equipment," broadly defined to include "personal computers . . . library resources, telephones, facsimile machines, photocopiers, [office supplies." There is a vague promise that the policy may be narrowed in the future, but it is the quoted language the Judicial Conference is being asked to approve on Sept. 11.

Not surprisingly, the proposed policy has raised a public furor. This has so worried the policy's proponents that Judge Edwin Nelson, chairman of the Judicial Conference's Automation and Technology Committee, took the unprecedented step of writing to all federal judges to reassure them that the proposed policy is no big deal. I asked that my response to Judge Nelson be distributed to federal judges on the same basis as his memo, but my request was rejected. I must therefore take this avenue for addressing my judicial colleagues on a matter of vital importance to the judiciary and the public at large.

The policy Judge Nelson seeks to defend as benign and innocuous would radically transform how the federal courts operate. At the heart of the policy is a warning--very much like that given to federal prisoners--that every employee must surrender privacy as a condition of using common office equipment. Like prisoners, judicial employees must acknowledge that, by using this equipment, their "consent to monitoring and recording is implied with or without cause." Judicial

opinions, memoranda to colleagues, phone calls to your proctologist, faxes to your bank, e-mails to your law clerks, prescriptions you fill online--you must agree that bureaucrats are entitled to monitor and record them all.

This is not how the federal judiciary conducts its business. For us, confidentiality is inviolable. No one else--not even a higher court--has access to internal case communications, drafts or votes. Like most judges, I had assumed that keeping case deliberations confidential was a bedrock principle of our judicial system. But under the proposed policy, every federal judge will have to agree that court communications can be monitored and recorded, if some court administrator thinks he has a good enough reason for doing so.

Another one of our bedrock principles has been trust in our employees. I take pride in saying that we have the finest work force of any organization in the country; our employees show loyalty and dedication seldom seen in private enterprise, much less in a government agency. It is with their help--and only *because* of their help--that we are able to keep abreast of crushing caseloads that at times threaten to overwhelm us. But loyalty and dedication wilt in the face of mistrust. The proposed policy tells our 30,000 dedicated employees that we trust them so little that we must monitor all their communications just to make sure they are not wasting their work day cruising the Internet.

How did we get to the point of even considering such a draconian policy? Is there evidence that judicial employees massively abuse Internet access? Judge Nelson's memo suggests there is, but if you read the fine print you will see that this is not the case.

Even accepting the dubious worst-case statistics, only about 3% to 7% of Internet traffic is non-work related. However, the proposed policy acknowledges that employees are entitled to use their telephone and computer for personal errands during lunchtime and on breaks. Because lunches and breaks take up considerably more than 3% to 7% of the workday, we're already coming out ahead. Moreover, after employees were alerted last March that downloading of certain files put too much strain on the system, bandwidth use dropped dramatically. Our employees have shown they can be trusted to follow directions.

What, then, prompted this bizarre proposal? The answer has nothing to do with bandwidth or any of the other technical reasons articulated by Judge Nelson. Rather, the policy became necessary because Leonidas Ralph Mecham, director of the Administrative Office of the U.S. Courts, was caught monitoring employee communications, even though the Judicial Conference had never authorized him to do so. Unbeknownst to the vast majority of judges and judicial employees, Mr. Mecham secretly started gathering data on employee Internet use. When the Web sites accessed from a particular computer affronted his sensibilities, Mr. Mecham had his deputy send a letter suggesting that the employee using that computer be sanctioned, and offering help in accomplishing this. Dozens of such letters went out, and one can only guess how many judicial employees lost their jobs or were otherwise sanctioned or humiliated as a consequence.

When judges of our circuit discovered this surreptitious monitoring, we were shocked and dismayed. We were worried that the practice was of dubious morality and probably illegal. We asked Mr. Mecham to discontinue the monitoring. Rather than admitting fault and apologizing, Mr. Mecham dug in his heels. The monitoring continued for most of the country until Mr. Mecham was ordered to stop by the Judicial Conference Executive Committee.

Hell hath no fury like a bureaucrat unturfed. In a fit of magisterial petulance, Mr. Mecham demanded that his authority to monitor employee communications be reinstated without delay. A compliant Automation Committee hastily met in secret session to draft the proposed policy, pointedly rejecting all input from those who might oppose it. In their hurry to vindicate Mr. Mecham's unauthorized snooping, the committee short-circuited the normal collegial process of deliberation and consultation.

Salving Mr. Mecham's bureaucratic ego, and protecting him from the consequences of his misconduct, is hardly a basis for adopting a policy that treats our employees as if they live in a gulag. Important principles are at stake here, principles that deserve discussion, deliberation and informed debate. As Chief Judge James Rosenbaum of Minnesota has stated, "giving employers a near-Orwellian power to spy and snoop into the lives of their employees, is not tenable." If we succumb to bureaucratic pressure and adopt the proposed policy, we will betray ourselves, our employees and all those who look to the federal courts for guidance in adopting policies that are both lawful and enlightened.

I therefore suggest that all federal judges reading these words--indeed all concerned citizens--write or call their Judicial Conference representatives and urge them to vote against the proposed policy. In addition, we must undo the harm we have done to judicial employees who were victims of Mr. Mecham's secret, and probably illegal, snooping. The Judicial Conference must pass a resolution that offers these employees an apology and expungement of their records.

Moreover, we should appoint an independent investigator to determine whether any civil or criminal violations of the Electronic Communications Privacy Act were committed during the months when 30,000 judicial employees were subjected to surreptitious monitoring. If we in the judiciary are not vigilant in acknowledging and correcting mistakes made by those acting on our behalf, we will surely lose the moral authority to pass judgment on the misconduct of others.
Mr. Kozinski is a judge on the Ninth U.S. Circuit Court of Appeals in California. His unmonitored e-mail address is kozinski@usc.edu.

EXHIBIT 4

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.

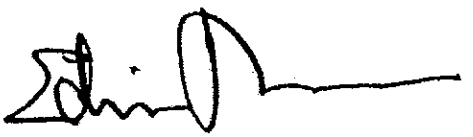
- Under the present state of the law, the federal judiciary is governed by the provisions of the Electronic Communications Privacy Act (the "ECPA"). This amendment would, in my opinion, call into question the status of the judiciary under the ECPA, while leaving intact provisions of law that allow other 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