2002

Internet Monitoring Of Federal Judges: Striking A Balance Between Independence And Accountability

Hardeep Kaur Josan

Sapna K. Shah

Follow this and additional works at: http://scholarlycommons.law.hofstra.edu/hlelj

Part of the Law Commons

Recommended Citation

This document is brought to you for free and open access by Scholarly Commons at Hofstra Law. It has been accepted for inclusion in Hofstra Labor and Employment Law Journal by an authorized administrator of Scholarly Commons at Hofstra Law. For more information, please contact lawcls@hofstra.edu.
INTERNET MONITORING OF FEDERAL JUDGES: STRIKING A BALANCE BETWEEN INDEPENDENCE AND ACCOUNTABILITY

I. INTRODUCTION

Here’s an everyday story: another group of employees discovers that they are being monitored at work for signs of . . . downloading music, watching streaming video and hunting pornography. They rebel, insisting that their bosses turn off the monitoring software or they will go to court for violation of privacy. That would be a short trip, because these complainants are themselves senior judges of the United States Court of Appeals.¹

It has been debated and resolved that private employers are permitted to monitor the Internet use² of their employees. The current controversy surrounds the manner in which federal judges’ Internet use is to be monitored, if at all. Judges oppose being monitored and claim that it violates the Electronic Communications Privacy Act of 1986 (“ECPA”),³ which makes it illegal to intercept any “wire or electronic communication” without notice.⁴

This note explores the Internet use policies recommended by the Committee on Automation and Technology of the Judiciary Conference of the United States (“CAT”), and later adopted by the Judicial Conference of the United States (“Judicial Conference”). Part II examines the recommendations (“Initial Policy”) proposed by CAT and judges’ opposition to this policy. Part III discusses the revised proposal (“Adopted Policy”) that was subsequently adopted on an interim basis. Part IV analyzes the Adopted Policy’s advantages and disadvantages. More specifically, Part IV addresses the factors of judicial

². For the purposes of this note, Internet use includes the use of electronic mail (“e-mail”).
independence, judicial accountability and judicial security, which should be considered in adopting any policy that monitors judges. Part V examines possible resolutions to the Adopted Policy, including alternative measures necessary to provide sufficient notice and consent to the Adopted Policy.

II. BACKGROUND OF THE ADOPTED POLICY

The Administrative Office of the Courts ("AO") implements policies created by the Judicial Conference, such as appropriate Internet use policies. Prior to the adoption of an Internet use policy, judges held that employees had no reasonable expectation of privacy regarding their Internet use. The CAT recommended the Initial Policy, which provided for the monitoring of Internet use, of all judiciary employees, including judges. Judges have publicly disfavored this Initial Policy.

A. Judicial Conference of the United States

The Judicial Conference is the body that initiates policies for the federal court system. Created by Congress in 1922, the Judicial Conference has the "ultimate authority over the internal operation of the federal courts . . ." The Chief Justice of the United States Supreme Court is the presiding officer of the Judicial Conference. The chief judges from the thirteen courts of appeals, a district judge from each of the twelve circuits and the chief judge of the Court of International Trade constitute the members of the Judicial Conference. The Judicial Conference meets biannually to discuss administrative and policy issues
with respect to the court system. Additionally, it makes recommendations to Congress regarding legislative aspects of the Judiciary.

As one of its duties, the Judicial Conference must submit suggestions to the various courts in the "interest of promoting uniformity of management procedures and the expeditious conduct of court business . . . ." The Judicial Conference also supervises the Director of the AO, who in turn functions as the administrative officer of the courts. The Director's duties include "supervising all administrative matters relating to the offices of the clerks and other clerical and administrative personnel of the courts . . . ."

B. How Judges Viewed Issues of Privacy Before the Initial Policy

Employers are concerned that they may be subject to civil or criminal liability as a result of employee misuse of the Internet. Employers prefer to diminish the possibility of potential abuse by occasionally monitoring employees' use of the Internet. Furthermore, upon termination of employment, employers have access to the employee's e-mail account and can respond to e-mail that continues to arrive.

In Smyth v. Pillsbury Co., a federal district court dismissed an invasion of privacy case by an employee who was fired for statements he made in an e-mail to his supervisor. The court held that even though employers assured e-mail would remain privileged and confidential, employees still had no reasonable expectation of privacy. The court reasoned that once an employee communicates to a third party over an e-

14. Id.
15. Id.
17. Id.
20. Id.
21. Id.
23. Id. at 101.
24. Id.
mail system, which is used by the entire company, reasonable expectations of privacy disappear.\textsuperscript{25} Since judges are struggling to preserve their own privacy in the workplace, decisions like Smyth may become rare.\textsuperscript{26}

In \textit{Bourke v. Nissan Motor Corp.},\textsuperscript{27} the employer randomly accessed one of its employee’s e-mail messages that contained personal and sexual statements.\textsuperscript{28} The employee sued the employer for invasion of privacy and for violating the ECPA.\textsuperscript{29} The court held that employees had no reasonable expectation of privacy in using e-mail because all employees had signed waivers.\textsuperscript{30} The waivers stated that employees must limit the use of company computers to business-related matters.\textsuperscript{31}

In addition, courts have found that public employees lack a reasonable expectation of privacy.\textsuperscript{32} In \textit{United States v. Simons},\textsuperscript{33} a government employee was charged with violating federal laws against child pornography after pornographic materials were found on the employee’s computer.\textsuperscript{34} The court held that government employees do not have a reasonable expectation of privacy with respect to information stored in their computers at work.\textsuperscript{35}

\textbf{C. Recommendations Initiated by the Committee on Automation and Technology}

The CAT recommended that the Judicial Conference consider the following proposals.\textsuperscript{36} First, allow for the decentralization of Internet

\textsuperscript{25} Id.
\textsuperscript{27} No. BO68705 (Cal. Ct. App. July 26, 1993).
\textsuperscript{28} Modelski, \textit{supra} note 19.
\textsuperscript{29} Id.
\textsuperscript{30} Id.
\textsuperscript{31} Id.
\textsuperscript{32} Id.
\textsuperscript{33} 206 F.3d 392 (4th Cir. 2000).
\textsuperscript{34} Id. at 395.
\textsuperscript{35} Id. at 398; \textit{see also} Wasson \textit{v. Sonoma County Junior Coll.}, 4 F. Supp. 2d 893 (N.D. Cal. 1997) (holding that a policy giving the public employer the right to access all information stored on its computer defeats an employee’s reasonable expectation of privacy); United States \textit{v. Monroe}, 52 M.J. 326 (C.A.A.F. 2000) (opining that an Air Force sergeant does not have a reasonable expectation of privacy in his workplace e-mail account because e-mail was used only for official business and because the network banner notified each employee upon logging on that the use of the e-mail was subject to monitoring).
\textsuperscript{36} Initial Policy, \textit{supra} note 7.
access from a national level to individual courts. Such decentralization would give each court considerable autonomy in accordance with policies and guidelines set at the national level. Second, permit a unit of the AO to control the inappropriate use of government resources. Third, give individual courts the responsibility of enforcing appropriate policies. Fourth, require the AO to distribute the proposals, approved by the Judicial Conference, to all judicial branch employees requesting each court to display an on-screen banner notice. Prior to accessing the Internet, each court would be disclosing that the use of the computer system is subject to the interim policy, and that its contents may be viewed and recorded. The banner notice will explicitly state that the employee’s use of the system constitutes consent to viewing and recording, and that uses inconsistent with the policy may result in disciplinary action. Finally, direct the AO to take appropriate steps to block traffic from Internet services such as Napster, Glacier and Quake, involving computers connected to the Data Communications

37. Id.
38. Id.
39. Id.
40. Id.
41. Initial Policy, supra note 7.
42. Id. The interim policy is the model policy adopted by the executive branch and revised by the CAT. Id. The CAT tailored the executive branch policy to the judicial system as a national minimum standard. Id. In promulgating this policy, the CAT relied on the Recommended Executive Branch Model Policy:

Executive Branch employees do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time, including accessing the Internet, using E-mail . . . . By using Government office equipment, executive branch employees imply their consent to disclosing the contents of any files or information maintained or [that] pass-through Government office equipment.

43. Initial Policy, supra note 7.
44. Id.
46. Glacier is a “back door program” that permits third parties to acquire control of a desktop computer or operating system without consent of the user and allows them to manipulate the computer’s hardware. ADDENDUM TO INITIAL POLICY, supra note 18, at 13.
47. Quake is a game program that allows third parties to gain access to a computer desktop during a game session and control the contents of the desktop. Id.
Network ("DCN"), and to delegate to a committee the authority to block other tunneling protocol that may cause security breaches.  

D. The Goals of Adopting the Initial Policy

The Judicial Conference has been debating whether to approve or dismantle the computer program that will subject judicial employees, including judges, to monitoring their Internet use at work. The CAT issued a policy to allow federal courts to monitor Internet use in order to deter inappropriate usage, e.g., downloading music and pornography or playing games. The Initial Policy sought to prohibit Internet use that congests or disrupts normal service and that generates extraneous governmental expense. The Initial Policy clearly stated that court employees using the computer system would be subject to monitoring, and therefore have no reasonable expectation of privacy.

The aim of the Initial Policy is twofold: (1) to secure the courts' computers by protecting them from viruses and hackers and (2) to ensure that employees do not waste time browsing the Internet for leisure. Dick Carelli, a spokesman for the AO, stated that the American taxpayer does not want "government employees us[ing] government computers on government time for pursuits that are obviously not job-related . . . ."

E. How the Software Works

The federal judiciary implemented a closed computer system enabling judges and other judiciary employees to communicate.

48. Initial Policy, supra note 7.
49. Rosen, supra note 11.
52. Krebs, supra note 50.
53. A hacker is defined as "a computer user who attempts to gain unauthorized access to files and various systems," WEBSTER'S NEW WORLD COLLEGE DICTIONARY 638 (4th ed. 2001).
54. Maria M. Perotin, Privacy Matters: E-mail Decision May Send Strong Signal, FORT WORTH STAR TELEGRAM, Oct. 8, 2001, at 15.
55. Id.; MODEL POLICY, supra note 42, at 2 ("Taxpayers have the right to depend on their Government to manage their tax dollars wisely and effectively. Public confidence in the productiveness of government is increased when members of the public are confident that their government is well managed and assets are used appropriately.").
internally. The system was designed to block third parties from gaining access into the judiciary's computer system. Despite the exclusion of third parties Leonidas Ralph Mecham, the Director of the AO, told the CAT that judges had been complaining about poor Internet response time. After investigating such complaints, Director Mecham discovered that the increased response time during business hours was due to the fact that three to seven percent of the judiciary's browser traffic involved streaming media, e.g., audio and video downloads. Since the Internet slowdown was due to non-work related Internet use that imposed a financial burden on the judiciary, Director Mecham installed software to identify the potential hackers.

The software recorded downloads of mpeg movie files and MP3 music files. It also notified federal judiciary employees, each time they logged onto the Internet, via an electronic banner, that they should expect no privacy. The software generated reports that were sent to Director Mecham's deputy, Clarence Lee, who determined whether the music files were inappropriate. If the files were inappropriate, Lee would send a letter to the chief judge of that circuit identifying the files, the computers from which they were downloaded and would recommend disciplinary action.

57. Id.
58. Rosen, supra note 11.
59. Id.
60. Id.
61. Id.
63. Id.; Krebs, supra note 50; ADDENDUM TO INITIAL POLICY, supra note 18, at 11. The Addendum recommended
[t]hat Judicial Conference require the Administrative Office to disseminate to all judicial branch employees now and hereafter hired, and to request each court prominently to display on screen prior to access of the DCN and the Internet, a banner notice clearly and conspicuously disclosing that the contents of the use may be viewed and recorded, that the employee's use of the system constitutes consent to such viewing and recording . . .
64. Rosen, supra note 11.
65. Id.
F. Opposition to Adoption of an Internet Use Policy

Although many critics of the Initial Policy acknowledge the "government's legitimate interest in protecting its computer resources from internal abuse and external threats[,]" the source of contention lies in the manner chosen by the CAT to achieve such goals. More specifically, most critics were outraged with the proposed policy that all judiciary employees, including judges, must waive all expectations of privacy in communications made when using office equipment, including computers.

Judges have criticized the monitoring on grounds that it is an invasion of privacy and that it may violate the ECPA. Judges stated that if e-mail is analogous to a phone call, then software that monitors it without notice to the parties, violates the anti-wiretapping regulations. However, if e-mail is analogous to a postcard, then it is open for everyone to read, and individual privacy is not jeopardized.

In 1999, the AO installed the monitoring software in New Orleans, San Francisco and Washington. The Ninth Circuit protested the monitoring of its computers. The judges temporarily disconnected the monitoring software claiming that it was illegal. Judge Alex Kozinski, of the Ninth Circuit, claimed that the monitoring violated the ECPA. Judge Kozinski further noted that adoption of the monitoring would

67. Alex Kozinski, Privacy on Trial, WALL ST. J., Sep. 4, 2001, at A22. Ninth Circuit Judge, Alex Kozinski, addressed this article as an "open letter to federal judges." Id.
70. Id.
71. Lewis, supra note 56. See Jim Tyre, Judicial Monitoring: The Bureaucrat Blinks, Privacy Wins (Sept. 8, 2001), at http://www.censorware.net/article.pl?sid=01/09/08/0420219&mode=nested&tid=1, for a discussion of the AO’s implementation of the new “censorware” on the federal judicial system.
73. Id.
74. Michael Fraase, Even Federal Judges Subject to Workplace Privacy Issues (Aug. 8, 2001), at http://www.farces.com/farces/997291903/index.html. Judge Kozinski suggested that an independent investigator be hired to determine whether any civil or criminal violations of the ECPA were committed when 30,000 judicial employees were subjected to surreptitious monitoring for several months. Kozinski, supra note 67 (“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.”).
“betray ourselves, our employees and all those who look to the federal courts for guidance in adopting policies that are both lawful and enlightened.”

The Initial Policy would require computer users to give up all privacy. "Turn on your computer, and everything on it, your recipes, your telephone book, anything you type on it becomes accessible by the employer . . . ." Judge Kozinski noted that “[t]his kind of intrusion is uncivilized.” Some employees use the Internet on their lunch hours for personal purposes, such as filling prescriptions or checking bank account balances. Such activities should remain private. Otherwise, a judiciary employee’s computer is an open book. Employees should not have to give up their rights without a showing of necessity.

As the most vocal critic, Judge Kozinski analogized the proposed policy to the “signs at federal prisons warning inmates that their phone conversations could be monitored.” For Judge Kozinski, judiciary employees, just like prisoners, would have to acknowledge that by using the office equipment their consent would be implied with or without cause. He premised his objections to monitoring on two bedrock principles of the judicial system; case deliberations should be kept confidential and loyal judicial employees should be trusted. Placement of this trust in judicial employees parallels such employees’ willingness to uphold the integrity of the judiciary. For example, after employees were told that downloading certain files put a strain on the system, there was a dramatic decrease in bandwidth. The Initial Policy suggests that judicial employees are not trusted, and therefore their communications

76. Dolan, supra note 62.
77. Id. (quoting Judge Kozinski).
78. Joan Biskupic, Judges Debate Own Privacy, USA TODAY, Sept. 7, 2001, at 1A.
79. Id.
80. Id.
81. Lewis, supra note 56.
82. Id.
84. Kozinski, supra note 67 (“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.”).
85. Kozinski, supra note 67. The Model Policy also upholds this principle. MODEL POLICY, supra note 42, at 2 (“The relationship between the Executive Branch and the employees who administer the functions of the Government is one based on trust.”).
86. Kozinski, supra note 67.
must be monitored. "[L]oyalty and dedication wilt in the face of mistrust." According to Judge Kozinski, the adoption of such a policy involves important principles, and deserves "discussion, deliberation and [an] informed debate." Furthermore, Kozinski claimed that "[i]f we take an extreme position as employers, then when the same issue comes up in a case where we have to decide as judges, we're more likely to approve the extreme position. So in a way we've prejudged the issue by conduct."

It is argued that deliberation did not take place prior to the formulation of the CAT's Initial Policy. Judge Kozinski noted that Director Mecham's investigation found that only about three to seven percent of Internet traffic is non-work related. Given that employees are entitled to use their telephone and computer for personal errands during non-work time, e.g., lunches and breaks, and that non-work time takes up more than three to seven percent of the workday, the judiciary is "already coming out ahead." In an interview, Kozinski stated that, in the federal workforce,

your telephone is owned by the government, but you don't expect them to tape phone conversations with your mother . . . . Your desk is owned by the government, but you don't expect them to rifle through it and make a copy of your diary. To say—just because the computer is owned by your employer—that you have no private space in it is going in the wrong direction.

He further criticized that judges are mature enough to preside over death penalty cases, decide whether individuals are sent to prison and how much money one is awarded, but cannot be trusted with using a web browser.

Judge Edith Jones, of the Fifth Circuit, has also voiced objections to the Initial Policy. According to her, the Initial policy "bespeak[s] a

87. Id.
88. Id.
89. Id.
91. Kozinski, supra note 67.
92. Id.
93. Id.
96. Letter from Honorable Edith H. Jones, Justice, United States Court of Appeals for the
solution in search of a problem.” She objected to the policy on several grounds. First, the recommendations seek to centralize decision-making about Internet and computer usage policies in a single national body, which is contrary to the longstanding trend toward decentralized court management. Thus, the policy confers great discretionary powers to the AO that should, instead, be retained by each judge’s own chambers. Second, the recommendations would “advise judicial branch employees that no one, including judges, has any expectation of privacy in his use of government computers for Internet or e-mail purposes . . . [which] is the equivalent of sanctioning wiretapping of telephones or searches of office files to ‘prevent unauthorized use of government property.’” Judge Jones noted that the proposal makes it possible not only for judicial bureaucrats to monitor computer traffic in judges’ chambers, but also for individuals with no links or loyalty to the judiciary to monitor computer use by judges. Finally, since the CAT’s report cites to only a few dozen examples of misuse among 30,000 judiciary employees, the recommended monitoring program seems highly disproportionate. There appears to be no sufficient reason why less intrusive means would not suffice to discourage Internet or computer misuse.

Chief Judge Mary Schroeder, of the Ninth Circuit, was concerned that the policy on Internet use implemented by the court was unclear. Chief Judge Schroeder stated that judges want to reach a “responsible, common sense resolution . . . without further acrimony.” She further noted that judges were troubled about “the propriety, and even the legality, of monitoring Internet usage by court employees’ without their

---

97. Id.
98. Id.
99. Id.
100. Id.
101. Krebs, supra note 50.
102. Jones Letter, supra note 96.
103. Id. For example, in March, after the monitoring program became publicized, “the Executive Committee issued a communiqué regarding appropriate usage that was widely disseminated throughout the judiciary . . . [Thereafter] bandwidth usage immediately and dramatically declined in response to that communiqué.” Id.
consent.” She urged judicial leaders to focus on detecting hackers, rather than monitoring judicial employees.

Another opponent of the Initial Policy, Ninth Circuit Senior Judge Alfred Goodwin, referred to the monitoring as “a busybody project by a few misguided bureaucrats.” Judge Michael Luttig, of the Fourth Circuit, stated that all judges “should be concerned when anyone, especially the government, is able, whenever it wishes, to monitor our use of the Internet.” An anonymous district court judge has handled cases requiring visits to pornographic websites. Therefore, judges and clerks may have a legitimate reason to view these sites.

The Federal Judges Association opposed the monitoring of electronic communications of judges’ chambers because it is a threat to judicial independence. An official at the United States Supreme Court, which is not governed by the actions of the Judicial Conference, stated that “the Court does have a computer use policy which employees sign and acknowledge when they come on board.” Internet access is limited to a few computers at the Court and most of them are not connected to the Internet because of security reasons.

The Executive Director of the Electronic Privacy Information Center (“EPIC”), Marc Rotenberg, wrote to the Judicial Conference urging it not to monitor the computer usage of judiciary employees. He argued that giving notice to judges does not resolve the Fourth Amendment issues raised when judiciary networks are monitored. The Electronic Frontier Foundation (“EFF”) opposed the monitoring on the grounds that if judges cannot be trusted to use judicial computers properly, then they should not be trusted to administer the courts.

106. Tyre, supra note 71.
107. Egelko, supra note 94.
109. Id.
110. Id.
111. Id.
112. The Federal Judges Association is an organization that represents 85% of federal judges. Gordon, supra note 26.
113. Id.
114. Groner, supra note 108. The official at the United States Supreme Court has refused to detail the policy implemented at the United States Supreme Court and the amount of time it has been in place. Id.
115. Id.
116. EPIC ALERT, supra note 68.
117. Id. See infra Part IV.A.
The EFF also argued that privacy concerns are raised when a non-judicial commercial company is monitoring judicial Internet use, case-related materials and private correspondence within the court system.119

Lawmakers have also opposed unrestricted judicial monitoring.120 Senator Charles Schumer (D-N.Y.) and Representatives John Conyers, Jr. (D-Mich.) and Howard Berman (D-Cal.) question the legality of such monitoring. They claim that even if the proposal is legal, the unrestricted monitoring would “lower employee morale, create an atmosphere of distrust and interfere with employees' reasonable expectation of privacy.”121 Representative Berman, a member of the House of Judiciary Subcommittee on Courts, said that he would “oppose any efforts by the Judicial Conference to systematically monitor the electronic communications and Internet use of judicial employees.”122 Although he deemed it appropriate for a supervisor to monitor the Internet use of an employee in certain situations, he found it inappropriate for the courts to monitor Internet use of employees because judges would face the task of ruling on issues of employee privacy.123

In response to the objections raised in opposition to the monitoring, David Sellers, the chief spokesman for the AO, stated that all the concerns were overblown.124 According to Sellers, “[t]here is not, there never has been, and there is not expected ever to be a situation in which e-mail will be monitored.... All that was ever monitored was the transfer of large files, big movements of information that clog up the bandwidth.”125

District Judge Edwin Nelson of Birmingham126 said that the “Constitution gives judges independence in decision-making... [but] 'does not place us above the law or free us from responsibility and accountability that taxpayers have a right to expect of public servants.'”127 J. Harvie Wilkinson III, Chief Judge of the Fourth Circuit,

119. Id.
120. Gordon, supra note 26.
121. Id.
123. Id.
125. Id.
126. Judge Nelson is the chairman of the CAT. Kozinski, supra note 67.
127. Weisman, supra note 51. In November 2001, California Judge Ronald Kline was charged with possession of child pornography. See Barbara Whitaker, Judge Facing Pornography Charges is Unopposed on Ballot, N.Y. TIMES, Mar. 2, 2001, at A10. The charge arose from information provided by individuals who surf the Internet in search of child pornographers. Id. A hacker infected the judge's computer with a virus and made an unauthorized copy of his hard drive. Id.
stated that there is a likelihood for abuse of the Internet in the workplace or a decrease in employee productivity. Moreover, he stated that the public has the right to expect that computers, which are purchased with taxpayers’ money, should be used for public business. Chief Judge Wilkinson also claimed that “special precautions” are taken to ensure that the “confidences of judicial communications are preserved.”

III. THE ADOPTED POLICY

The Adopted Policy has been approved by the Judicial Conference on an interim basis. The policy will be in effect only until the Judicial Conference is able to agree upon a permanent policy. The Adopted Policy is modeled after the General Services Administration’s proposal and guidance on the appropriate use of government equipment.

A. The Judicial Conference’s Adopted Policy

Director Mecham, in a letter to Judge Nelson, Chairman of the CAT, suggested that the two most objectionable recommendations be removed from the policy. The objected recommendations pertained to employees waiving their privacy rights and that all computers display a banner message. Director Mecham pointed out that judges have legitimate interests in protecting the privacy of their communications. He further noted that complete abandonment of privacy expectations was not necessary to achieve the goal of managing judiciary resources. Perhaps fearing that the Judicial Conference would not adopt the

Child pornography was found in the judge’s work and personal computers. Id. As of August 10, 2002, Judge Kline was under house arrest and awaiting trial in federal court. Judge Pleads Not Guilty to Child Sex Charges, L.A. TIMES, Aug. 10, 2002, § 2, at 3.

128. Groner, supra note 108.
129. Id.
130. Id.
132. Id.
133. Id.
134. Fax from Leonidas Ralph Mecham, Director of AO, to Honorable Edwin L. Nelson, Chairman of the CAT, (Sept. 6, 2001), at http://censorware.net/documents/mecham-20010906.pdf [hereinafter Mecham Fax].
135. Id.
136. Id.
137. Id.
proposition, the CAT revised its recommendations from unrestricted to limited monitoring. 138

On September 19, 2001, the Judicial Conference adopted the revised recommendations proposed by the CAT. 139 The approval calls for the following actions: (1) decentralization of Internet access to individual courts such that all computers connected to the DCN access the Internet through national Internet gateways under the control of the AO; (2) give individual courts the responsibility of enforcing appropriate use policies, which the AO may examine and comment upon; (3) adopt the model use policy developed by the Federal Chief Information Officers Council as a national minimum standard defining appropriate Internet use; 140 (4) give the AO the authority to take appropriate steps to block such traffic as Napster, Glacier and Quake from computers connected to the DCN, and give the CAT the authority to block other tunneling protocol that may cause security breaches; (5) no monitoring of employees' e-mail use and no waiver of all expectations of privacy. 141

The Judicial Conference decided to omit from the newly Adopted Policy the proposition that judiciary employees have no right to privacy when they use the Internet. 142 While the policy does not guarantee any specific right to privacy at the workplace for the judiciary, privacy experts view the omission as a victory for judges who had fought to keep e-mail communication private. 143 In fact, Judge Kozinski, the fiercest opponent of the original recommendation, was pleased with the outcome primarily because "there's no monitoring of individual computers, and

138. Mecham Fax, supra note 134.

139. Recommendation Approval, supra note 131. The policies were supposed to be debated at a regular meeting of the conference on September 11, 2001, but the meeting was canceled due to the terrorist attacks on New York City and the Pentagon. Mauro, supra note 83. Instead of waiting for another conference, Chief Justice William Rehnquist, decided to submit the issue to the Judicial Conference for a vote by mail. Id.

140. Inappropriate use of judiciary computers includes:

the creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials... materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited... any personal use that could cause congestion, delay or disruption of service to any government system or equipment... any use that could generate more than minimal additional expense to the government....

Recommendation Approval, supra note 131.

141. Recommendation Approval, supra note 131. The Approval explicitly excludes Section F of the MODEL POLICY, which allows for unrestricted monitoring. Compare Recommendation Approval, supra note 131 with MODEL POLICY, supra note 42.


143. Id.
there’s not going to be.”

According to Judge Kozinski, “[i]t was a serious mistake for Mr. Mecham and the [technology] committee to try to ram this through without the normal process of consultation and deliberation that has been the hallmark of judicial governance . . . . I’m glad they have recognized their error and withdrawn their highly intrusive proposal.”

B. Judicial Electronic Monitoring Modeled After the Executive Branch Plan

The electronic monitoring plan that the judicial branch has adopted is modeled after the plan that was recommended for employees of executive agencies. In 1999, the General Services Administration distributed to all executive branch agencies a proposed model policy regarding appropriate use of government equipment. The Federal Chief Information Officers Council developed the model policy after discussions with various government ethics, legal procurement and human resource experts. Since its formulation, the model policy has been adopted by approximately two-thirds of executive branch agencies. The remaining one-third have imposed more restrictive policies.

Limited personal use of government equipment by employees during non-working hours is authorized use of the government’s property. However, authorized use cannot interfere with official business and cannot involve more than minimal additional expense to the government. Inappropriate personal use of government equipment by employees is prohibited. Employees are responsible for ensuring

---

144. Groner, supra note 108.
145. Id. (alteration in original).
146. Recommendation Approval, supra note 131.
147. MODEL POLICY, supra note 42.
148. ADDENDUM TO INITIAL POLICY, supra note 18, at 9.
149. Id.
150. Id.
151. Id.
152. MODEL POLICY, supra note 42, at 4.
153. Id.
154. Inappropriate use of government equipment includes any personal use that causes delay, congestion or disruption of services to any government system. Id. Examples of inappropriate use include: accessing greeting cards or video, sound or other large file attachments that can disrupt the government’s system; creating, copying, or transmitting chain letters; illegal or offensive activities; creating, downloading, viewing, copying, or transmitting sexually explicit materials; creating, downloading, viewing, copying or transmitting materials relating to illegal gambling, illegal weapons, or terrorist activities; engaging in outside fund-raising activity; any use that causes more
that a false impression is not created when government computers are utilized for personal use.\textsuperscript{155} If the personal use may be interpreted to represent the agency, a disclaimer must be provided.\textsuperscript{156}

Government employees do not have a right to privacy when using the government computer \textit{at any time}.\textsuperscript{157} When an employee of the executive branch uses the government’s computer system, the employees implicitly consent to disclosure of the contents of their Internet use.\textsuperscript{158} For personal matters to remain private, employees should avoid using the government’s computer.\textsuperscript{159} Any communication made via the government’s computer is understood to be not secure, not private and not anonymous.\textsuperscript{160}

IV. ANALYSIS OF THE ADOPTED POLICY

This section briefly addresses the legality of monitoring the Internet use of employees through a short analysis of the Fourth Amendment and the ECPA. This section also endeavors to critique the Adopted Policy through a brief history of the judicial administrative system and the essential traits such administration must incorporate if it is to be successful. An examination of the Adopted Policy leads to the conclusion that it is deficient for a number of reasons.

A. Fourth Amendment Concerns

Government employees, specifically judicial employees, may find privacy protection of their Internet communications in the Fourth Amendment of the United States Constitution.\textsuperscript{161} The Fourth Amendment guarantees an individual’s privacy and dignity against certain intrusive acts by government entities, including government employers.\textsuperscript{162}

\textsuperscript{155} MODEL POLICY, \textit{supra} note 42, at 5.

\textsuperscript{156} \textit{Id.} Disclaimer stating that: “[t]he contents of this message are mine personally and do not reflect any position of the Government or my agency” would be deemed sufficient. \textit{Id.}

\textsuperscript{157} \textit{Id.} at 6.

\textsuperscript{158} \textit{Id.}

\textsuperscript{159} MODEL POLICY, \textit{supra} note 42, at 6.

\textsuperscript{160} \textit{Id.}

\textsuperscript{161} U.S. CONST. amend. IV. “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . .” \textit{Id.}

\textsuperscript{162} S. Elizabeth Wilborn, \textit{Revisiting the Public/Private Distinction: Employee Monitoring in}
In *Katz v. United States*, the Supreme Court established a two-prong test to determine whether the Fourth Amendment is violated: (1) the person must have a subjective expectation of privacy and (2) the expectation must be reasonable. Under the reasonable expectation of privacy test, an intrusion constitutes an unlawful search or seizure.

The Supreme Court first addressed the applicability of the Fourth Amendment to the privacy expectations of government employees in *O'Connor v. Ortega*. The Court held that government employees may have a reasonable privacy expectation at work. It further emphasized that a government employer is required to provide a legitimate work-related reason for the search. "[W]hether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis" and depends on "the operational realities of the workplace."

In *Chandler v. Miller*, the Supreme Court held that a government employer has to show the presence of a special need in order to engage in certain monitoring techniques. The Court struck down a state statute that imposed drug testing on political candidates. The Court held that the state failed to meet the "special needs" exception to the warrant and probable cause requirement of the Fourth Amendment. The state was unable to show any problem with drug abuse among state officials and further failed to show that its normal law enforcement methods were insufficient to adequately address any potential problem. *Chandler* and *O'Connor* together establish that "indiscriminate, groundless monitoring of personal conversations or activities will likely be held unreasonable and violative of the Fourth Amendment guarantee of privacy."

Given the "operational realities" of the judiciary, judiciary employees have a reasonable privacy expectation at work. In approving the Adopted Policy, the Judicial Conference arguably failed to articulate a legitimate work-related reason to justify the monitoring. Although a
computer slowdown is a work-related reason, it does not justify the breadth of the monitoring. Arguably, no special need existed to warrant the monitoring.\textsuperscript{176} Therefore, the indiscriminate application of the Adopted Policy is unreasonable and arguably violates the Fourth Amendment guarantee of privacy.

\textbf{B. Electronic Communications Privacy Act of 1986}

The ECPA\textsuperscript{177} prohibits the intentional monitoring of a facility without notice through an electronic communication service and the intentional accessing of a facility in order to obtain, alter or prevent authorized access through a wire or an electronic communication as an offense.\textsuperscript{178} ECPA section 2511(2)(a)(i) allows “a provider of wire or electronic communication service . . . to intercept . . . [a] communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service . . . .”\textsuperscript{179}

Relying on ECPA section 2511(2)(a)(i), employers justify monitoring on the grounds that it is necessary to prevent excessive personal use of the system.\textsuperscript{180} However, many people have argued that monitoring of judicial employees violates the ECPA.\textsuperscript{181} The ECPA allows interception of communications with the consent of only one of the parties involved.\textsuperscript{182} The CAT installed the monitoring program without notifying or securing the consent of judicial employees.\textsuperscript{183} For this reason, Judge Kozinski has argued that the Justice Department

\begin{footnotes}
\item[176] As Judge Kozinski noted, only three to seven percent of judiciary employees' Internet usage is not related to work. Kozinski, \textit{supra} note 67. These statistics may not suffice to constitute a special need.
\item[177] Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). Wire communication is defined as the transfer or transmission by means of a wire, cable or other connection from the beginning to the end. 18 U.S.C. § 2510 (2000). Intercept is defined as the acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device. \textit{Id.} Electronic, mechanical, or other device means any device or apparatus that can be used to intercept a wire, oral, or electronic communication. \textit{Id.} Person means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust or corporation. \textit{Id.} Judges are assumed to be included under the ECPA because they are governmental employees.
\item[178] \textit{Id.} § 2701.
\item[181] Rosen, \textit{supra} note 11.
\item[183] Rosen, \textit{supra} note 11.
\end{footnotes}
should initiate an investigation to determine whether any civil remedies are owed to judicial employees whose privacy rights may have been violated pursuant to the ECPA.\textsuperscript{184}

The merit of Judge Kozinski's contention is limited by the fact that the ECPA arguably does not provide effective protection for employee privacy. Although the ECPA does impose some restrictions on the manner or the extent of employee monitoring, its many exceptions swallow the rule. For example, ECPA section 2510(5)(a) allows a service provider to intercept "any wire or electronic communication service in the ordinary course of its business" which the user utilizes in such capacity.\textsuperscript{185} Employers with their own e-mail system may fall within the definition of a service provider, thereby allowing an employee’s Internet use to be monitored without violating the ECPA.\textsuperscript{186}

C. History of the Judicial Administrative System

Prior to 1939, the Department of Justice, an executive agency, performed the judiciary’s administrative duties,\textsuperscript{187} with each district judge responsible for court administration within the district.\textsuperscript{188} Beginning in the early 1900s, however, a movement towards an integrated administrative system began.\textsuperscript{189} In 1922, Congress created the Conference of Senior Circuit Judges, today known as the Judicial Conference, to "serve as the principal policy making body concerned with the administration of the United States Courts."\textsuperscript{190} Among other things, 28 U.S.C. section 331\textsuperscript{191} specifically grants the Judicial Conference the authority to "make a comprehensive survey of the condition of business in the courts of the United States.... submit

\hspace{1cm}\textsuperscript{184} Id.
\hspace{1cm}\textsuperscript{185} 18 U.S.C. § 2510(5)(a).
\hspace{1cm}\textsuperscript{186} Watson, supra note 180, at 86.
\hspace{1cm}\textsuperscript{187} Patrick Donald McCalla, Note: Judicial Disciplining of Judges is Constitutional, 62 S. CAL. L. REV. 1263, 1265 (1989) (describing administrative duties as budgeting, managing and paying salaries).
\hspace{1cm}\textsuperscript{188} Id.
\hspace{1cm}\textsuperscript{189} Harlington Wood, Jr., Judiciary Reform: Recent Improvements in Federal Judicial Administration, 44 AM. U. L. REV., 1557, 1561 (1995) (noting that such movement was initiated by judicial reformers like Roscoe Pound and William Howard Taft "to improve cumbersome court procedures and inefficient judicial administration").
\hspace{1cm}\textsuperscript{190} Judicial Conference, supra note 5. At its inception, the Conference of Senior Circuit Judges was composed of the chief justice and the chief judge of each circuit. McCalla, supra note 187, at 1265. In 1948, Congress enacted 28 U.S.C. § 331, changing the name of the Conference of Senior Circuit Judges to the Judicial Conference of the United States. Judicial Conference, supra note 5.
\hspace{1cm}\textsuperscript{191} 28 U.S.C. § 331 (2000).
suggestions and recommendations to the various courts to promote uniformity of management procedures and the expeditious conduct of court business.\textsuperscript{192} The Judicial Conference also participates in regulating judicial activities by promulgating ethical standards for judges and court personnel.\textsuperscript{193}

In 1939, Congress passed the Administrative Office Act, thereby completing the judicial administration reform movement.\textsuperscript{194} With this Act, Congress created the AO, which assumed the administrative duties previously performed by the Department of Justice.\textsuperscript{195} The Director of the AO, appointed by the Supreme Court, performs the statutory duties of the AO under the supervision and direction of the Judicial Conference.\textsuperscript{196} This arrangement reflects the view that the ultimate responsibility for managing the courts should remain with the Judicial Conference.\textsuperscript{197} The Judicial Conference adopts governing policies and procedures for the federal courts and the AO serves the Judicial Conference by implementing and executing such policies.\textsuperscript{198} The AO does not have direct management authority over the individual courts.\textsuperscript{199}

The Administrative Office Act of 1939 further strengthened judicial administration by creating Judicial Councils of the Circuits ("circuit councils").\textsuperscript{200} Each circuit council consists of an equal number of trial and appellate judges, with the circuit chief judge as chair.\textsuperscript{201} Circuit councils have the power to "take such action as is appropriate to assure the effective and expeditious administration of the business of the courts within the circuit."\textsuperscript{202} However, by 1985, the federal judicial administration system had become heavily centralized, thereby not

\textsuperscript{192} Id.
\textsuperscript{193} McCalla, supra note 187, at 1265.
\textsuperscript{194} Id. at 1265-66.
\textsuperscript{195} Wood, Jr., supra note 189, at 1562 (discussing that the administrative duties of the AO consist of procurement, personnel and payroll, managing the budget and accounting, statistics collection and reporting).
\textsuperscript{196} Id.
\textsuperscript{197} Id.
\textsuperscript{198} Id. at 1563.
\textsuperscript{199} Id. at 1564.
\textsuperscript{201} Id.
\textsuperscript{202} 28 U.S.C. § 372(c)(6)(B) (2000). "Thus, the administrative power, including the power to investigate judges, was not given to the United States Supreme Court, the Judicial Conference of the United States, or circuit or district courts, but to local independent administrative bodies comprised of judges." Wallace, supra note 200, at 348-49.
conforming to the "historical independence and autonomy of the federal courts in our constitutional system of government."\textsuperscript{203}

\textbf{D. The Necessity of Incorporating Essential Traits into the Judicial Administrative System}

The foregoing history and establishment of the judicial administrative system illustrates the unique structure of the employer-employee relationship within the judiciary. It further enables analyzing the problem of fitting judges and those who administer their conduct into pre-existing employer-employee models of supervision. The role that judges play in our society incorporates something more than one who works for another under an express or implied contract, thereby rendering the definition of "employee" inadequate as applied to judges.\textsuperscript{204} Similarly, the roles that the Judicial Conference and the AO play in administering the judiciary encompass something less than one who "controls and directs a worker under an express or implied contract," thereby rendering the definition of "employer" as inadequate as applied to the Judicial Conference and the AO.\textsuperscript{205} In other words, judges possess greater power than the definition for employee implies and the Judicial Conference and the AO possess less control than the definition of employer implies.

The inadequacy of applying the definitions of employer and employee within the judiciary leads to the conclusion that administration of the conduct of judges cannot be modeled after existing models of employee management. The unique setup and function of the judiciary cannot be compared to business entities or to other branches of the government. Therefore, any policy adopted to supervise the conduct of judges, including appropriate Internet use, must incorporate and balance the following traits: judicial independence; and judicial accountability and judicial security.

\begin{enumerate}
\item \textbf{Judicial Independence}

Judicial independence is one of the fundamental precepts upon which the American system of government was founded.\textsuperscript{206}
\end{enumerate}

\begin{footnotes}
\textsuperscript{203} Wood, Jr., \textit{supra} note 189, at 1564-65.
\textsuperscript{204} \textit{BLACK'S LAW DICTIONARY} 428 (7th ed. 2000).
\textsuperscript{205} \textit{Id.} at 430.
\end{footnotes}
The "independence of the judges is equally requisite to guard the Constitution and the rights of individuals from the effects of those ill humors which the arts of designing men, or the influence of particular conjunctures, sometimes disseminate among the people themselves ...." 207 The principle of judicial independence can be found in Article III, section 1 of the Constitution. 208 Article III, section 1 provides that "[t]he Judges, both of the supreme and inferior Courts, shall hold their Offices during good Behaviour, and shall, at stated Times, receive for their Services a Compensation, which shall not be diminished during their Continuance in Office."

The concept of judicial independence may be interpreted either narrowly, as a set of protections for judges, or broadly, as a guarantee of the integrity of the judicial system. 210 Judicial independence is a multifaceted principle. Its facets are illustrated in the different kinds of independence: (1) substantive independence; 211 (2) personal independence; 212 (3) collective independence; 213 and (4) internal independence. 214

2. Judicial Accountability

Judicial accountability encompasses the notion that judges need to be held accountable for their acts, both decisional and behavioral. This notion is premised on the idea that the public, as taxpayers, has the right to ensure that its money supports an efficiently run judiciary that upholds the law and the rights of the people. The principles of judicial accountability and judicial independence may be understood as

209. Id.
211. Also known as functional or decisional independence, substantive independence is defined as "making judicial decisions and exercising official duties subject to no other authority but the law." Maria Dakolias & Kim Thachuk, Attacking Corruption in the Judiciary: A Critical Process in Judicial Reform, 18 WIS. INT"L L.J. 353, 361 (2000).
212. Is defined as "adequately secured judicial terms of office and tenure." Id.
213. Is defined as "judicial participation in the central administration of courts." Id. at 361-62.
214. Is defined as "independence from judicial superiors and colleagues. Id. at 362.
The greater the independence of the judiciary, the greater the need for its accountability. If the judiciary is overly independent and unmonitored, then the concept of accountability will likely be compromised. Similarly, the stricter the standards of accountability imposed on the judiciary, the less independent it will remain. Although the two principles need to be properly balanced, one will always hold greater weight. The balance should be tilted in favor of judicial independence because such autonomy must be sufficiently present before any need for accountability arises. Thus, the importance of balancing the two principles with a tilt towards judicial independence is paramount to successful administration of the judiciary.

3. Judicial Security

Judicial security consists of the confidence and discretion inherent in decision-making. The functions performed by the judiciary in general, and by judges in particular, involve great degrees of confidentiality and impartiality. For judges to be fair and impartial in the adjudication of disputes assurances must be made as to the security of confidential information within chambers. Lack of such security, in the aggregate, could result in less confidence in the judiciary's ability to act as an impartial and fair adjudicator.

E. Deficiencies of the Adopted Policy

Judges had been complaining about the slow Internet response time of judiciary computers. As a result, a preliminary monitoring of judiciary employees' Internet use, by the AO identified the downloading of music and movies as the problem. The AO used this information as a basis for implementing an Internet use policy within the judiciary. Understandably, taxpayers do not want to fund judiciary employees' inappropriate use of the Internet. Even though judges have criticized the Internet use policy, they do recognize the government's legitimate interest in protecting its computers from internal abuse and external threats. While the Adopted Policy protects the foregoing interests, it does so at the expense of judicial integrity. To avoid
compromising judicial integrity, a less restrictive alternative should be sought. Therefore, the deficiencies of the Adopted Policy stem from its failure to properly balance the principles of judicial independence, judicial accountability and judicial security. The Adopted Policy’s deficiencies include its threat to impartial decision-making, its vague definition of inappropriate use, its lack of decentralization and its failure to provide notice to judiciary employees.

1. Threat to Impartial Decision-Making

Despite strong arguments for implementing a monitoring policy in the judiciary, strong reasons exist for dismantling the policy. First, since judges are held to a higher standard of conduct, they should regulate Internet use within the judiciary, not the AO. Second, monitoring would jeopardize judges’ duty of confidentiality by allowing third parties to view confidential information. Finally, monitoring may cause judges to have biases that would affect their decisions in future Internet monitoring cases. The judiciary’s integrity depends on its independence from outside influences. If a case is presented before a judge where an employer is monitoring an employee, the judge may identify with the employee and rule against the employer. Because judges themselves do not want to be monitored, they may rule in favor of employees’ privacy rights.220

2. Defining Inappropriate Use

Inappropriate use includes “[a]ny personal use that could cause congestion, delay, or disruption of service . . . [and] any use that could generate more than minimal additional expense to the government.”221 Given this definition, Director Mecham, notified the judicial system that the purpose of the new monitoring software is to enhance security, reduce non-official use and prevent “clogging the system.”222 A survey by the AO showed that three to seven percent of the judiciary’s Internet use consisted of radio and video broadcasts, which were unrelated to official business.223

---

220. Similarly, Judge Kozinski has argued that approval by federal judges of monitoring in the judiciary will “color” how monitored judges decide privacy cases in the future. Lewis, supra note 56.
221. MODEL POLICY, supra note 42, at 4-5.
222. Souza, supra note 69.
223. Neil Lewis, Rebels in Black Robes Recoil at Surveillance of Computers, N.Y. TIMES,
The definition of inappropriate use is overinclusive. A judge listening to the radio, which leads to a slow Internet response, could be deemed as an inappropriate use. However, the judge may be listening to background classical music that may improve productivity. It is difficult to draw the distinction between Internet radio broadcasts that result in slow Internet response and Internet radio broadcasts that enhance the work performance of judges. Therefore, using the Internet to listen to the radio should not be deemed inappropriate per se.

3. Lack of Decentralization

Although the Adopted Policy recognizes the importance of decentralization, which ultimately leads to greater judicial independence, it nonetheless, rests great oversight authority in the hands of the AO. The Adopted Policy expresses the possibility of decentralization and reaffirms the rule that individual courts are given responsibility to enforce Internet use policies. However, simultaneously, the AO is given authority to administer, manage and control operations and security at gateways, and to further oversee each court’s enforcement methods. Additionally, the CAT is given the authority to block “other tunneling protocol” that it determines may cause security breaches. Such grant of authority is quite ambiguous and arbitrary because it allows a committee that is not composed of judges to determine what should and should not be blocked. Judges and their law clerks are in a better position to know what web services are necessary for them to perform their judicial functions. For this reason, the Adopted Policy needs to address this tension between centralized and localized management.

4. Notice

The Adopted Policy is deficient in yet another way. The Privacy Expectations section of the Executive Model Policy has been omitted from the Adopted Policy. The deleted language required judges to give up all expectations of privacy when using the Internet within the.

224. Recommendation Approval, supra at 131.
225. Id.
226. Id.
227. Compare Recommendation Approval, supra note 131, with MODEL POLICY, supra note 42.
The omission does not guarantee or imply that there will be *no* monitoring of judges' Internet use. It simply means that before any monitoring, judges will be given notice. The issue of implementing notice has been recommitted to the CAT.  

It is unclear whether removing the Privacy Expectations section from the Adopted Policy implies that judiciary employees likewise have a reasonable expectation of privacy. The substance and extent of what constitutes a reasonable expectation of privacy is uncertain. Perhaps reasonableness should be defined in terms of "[t]he operational realities of the workplace," such as "actual office practices." It remains to be seen whether a forthcoming notice policy will incorporate, and properly balance, the concepts of judicial independence, judicial accountability and judicial security.

V. PRELIMINARY STEPS TOWARDS A RESOLUTION

The Adopted Policy presents a solution in search of a problem. The adoption of a policy to monitor judges' Internet use and e-mail is to conclude that such use has compromised the judiciary's adjudicative role. Among other things, the Adopted Policy purports to address concerns of adjudicative efficiency and waste of government resources. Concededly, these *are* legitimate and important interests that every taxpayer has a right to enforce if they are being threatened. Whether such resources are being abused to necessitate the implementation of the Adopted Policy is unclear. In approving the Adopted Policy, the Judicial Conference may have "short-circuited the normal collegial process of deliberation and consultation." Assuming the validity of this contention, the failure of the Adopted Policy stems primarily from its attempt to solve a non-existent, or at best, an ill-defined problem. A sound resolution cannot exist without a clear and comprehensive understanding of the problem.

A. Exclusion of Judges from the Adopted Policy

Assuming *arguendo* that the problems enumerated by the CAT do exist, the Adopted Policy is deficient for adopting the wrong means to

---

228. MODEL POLICY *supra* note 42.
correct such problems. The modest evidence supplied by the CAT reveals that inappropriate Internet use by judiciary employees causes congestion of Internet access and generates extraneous governmental expense.\(^2\)\(^3\)\(^4\)\(^5\) This evidence, even if valid, does not warrant curtailment of judges' Internet use because methods less intrusive on judicial independence may be available. For example, 30,000 employees exist in the federal judiciary, only 1,800 of whom are judges.\(^2\)\(^3\)\(^4\) Restricting the Internet use of the 28,200 non-judge employees is likely to have substantially the same effect upon eradicating the problems of congestion and waste as restricting the Internet use of all 30,000 employees, including judges. This would allow judges to retain a sense of confidence and independence without giving them the impression that they are not to be trusted. As Judge Kozinski noted, if judges are trusted enough to decide difficult cases, they should be trusted with using the Internet.\(^2\)\(^3\)\(^5\)

**B. The Sufficiency of Notice and Consent**

Sufficient notice and consent may be a possible compromise in making the Adopted Policy acceptable to all judiciary employees. A notice requirement would inform employees as to the amount of privacy that can be expected at work. To establish the degree of privacy, an employer should articulate its monitoring policy no later than on the date of hire.\(^2\)\(^3\)\(^6\)

An effective policy should explicitly state the communications that will be monitored by the employer. The policy should note that the computer system is the property of the workplace and should be used solely for work-related purposes. The policy should also detail prohibited Internet sites and clearly state that the employer could be held liable for any communication transferred through the Internet.\(^2\)\(^3\)\(^7\) Employees should be reminded that communications through the Internet and e-mail may be read or intercepted by third parties.\(^2\)\(^3\)\(^8\) Disciplinary action, such as discharge, could be imposed upon violators of the policy in order to ensure compliance.\(^2\)\(^3\)\(^9\) An on-screen message

\(^{233}\) Weisman, supra note 51.
\(^{234}\) Holland, supra note 75.
\(^{235}\) Wertheimer & Horsley, supra note 95.
\(^{237}\) Id.
\(^{238}\) Id.
\(^{239}\) Id.
could appear on the user’s computer every time the employee logs onto the network as a constant reminder of the implemented policy. Before a policy is executed, all judiciary employees should be aware of the amount of privacy to expect. The adoption of the Notice of Electronic Monitoring Act ("NEMA") may be a manner of providing such expectation of privacy.

1. Notice of Electronic Monitoring Act

In 2000, the NEMA was introduced in Congress but did not pass. The bill does not ban, or even limit, electronic monitoring. It merely requires prior notification by employers to monitor its employees’ electronic communications. The purposes of the bill are sound. Since e-mail is readily available, employers are concerned that employees may use it for unrelated work. As a corollary, employers are concerned that personal use of work computers may lead to potential liability, disclosure of sensitive information and a waste of time and resources. Employers hope that the notice will deter employees from using work computers for personal purposes during work time.

The NEMA requires an employer to give notice before monitoring, not before each instance of monitoring. The employer must give notice at the start of employment and continue to do so once a year as long as monitoring persists. The notice must be “clear and conspicuous” and given “in a manner reasonably calculated to provide actual notice ....” The notice must provide the following: (1) the form of communication or computer usage that is to be monitored; (2) the means by which such monitoring will be accomplished; (3) the kinds of information that will be monitored; (4) the frequency of the monitoring; and (5) the manner in which gathered information will be used.

240. Id.
242. Watson, supra note 180, at 80. The NEMA was introduced by Representatives Charles Canady (R-Fla.) and Bob Barr (R-Ga.), and Senator Charles Schumer (D-N.Y.). Id.
243. H.R. 4908.
244. Id.
245. Watson, supra note 180, at 81-82. According to a survey from the American Management Association, 45% of U.S. firms monitor their employees’ electronic communications, including e-mail, voice mail and Internet use. Id. at 82.
246. H.R. 4908.
247. Id.
248. Id.
249. Id.
The NEMA provides an exception to notice. The employer must have reasonable grounds to believe that; (1) the employee is engaged in conduct that violates the rights of another person; (2) the conduct involves "significant harm to the employer or other person;" and (3) the "monitoring will produce evidence of such conduct." The NEMA's purpose is to place employees on notice that monitoring will occur in order to prevent employees' misuse of the Internet and e-mail. The notice requirement would assist employees in separating personal material from work-related material. Employees would know what information is being monitored, and thus would be able to plan accordingly. Employees would be able to make decisions on what personal information to bring to the workplace.

2. Evaluation of the NEMA

There are many advantages to the NEMA. The notice requirement is fair because it allows for communication. Although employers cannot expect employees to refrain completely from handling personal matters at work, notice allows employers to state what is acceptable in the workplace. A reasonable policy might, for example, allow employees to use the Internet for personal matters before or after work and during lunchtime. Also, a notice requirement will not burden employers. A notice requirement will deter employees from engaging in activities that may lead to liability for the employers. Further, notice gives employees the opportunity to decide if they wish to continue working for the employer since notice is required before monitoring takes place.

There are also criticisms to the NEMA. The first criticism is that the NEMA does not require a certain method of giving notice to employees. It only requires that the notice be "clear and conspicuous"

250. Id.
251. H.R. 4908.
252. Watson, supra note 180, at 96.
253. Id.
254. Id.
255. Id.
256. Id. at 100.
257. Watson, supra note 180, at 100.
258. Id.
259. Id.
260. Id.
261. Id.
262. Watson, supra note 180, at 97.
and given "in a manner reasonably calculated to provide actual notice..." One solution to the criticism is to require written notice or a click-wrap agreement where the notice appears on the employee's computer. This would lead to minimal inconvenience to employers.

A second criticism of the NEMA is that it would raise the duty of care owed to employees. Employees might sue their employer based on a failure to monitor those communications specified in the employer's monitoring policy. Where an employer puts its employees on notice that it is monitoring e-mails, an employee sending harassing messages to another employee may give rise to employer liability. The harassed employee could argue that the employer should have caught the harassing employee through the monitoring of messages.

Critics of the NEMA further argue that a notice requirement could lead to more snooping by employers because it provides them with legitimate reasons to monitor. EPIC criticized the NEMA, stating that it would discourage an employee from making a legitimate invasion of privacy claim because employees would be effectively on notice.

VI. CONCLUSION

Continuous monitoring of judges' Internet use and blockage of sites deemed to be inappropriate assumes, without deliberation, that less restrictive measures will not suffice. The Adopted Policy fails to realize that judges need to be classified as a separate and distinct group from other employees. The status of judges gives them the right to expect a degree of trust without a bureaucratic eye watching over them. Judges are in a position to know what constitutes inappropriate Internet use because they are capable of interpreting language to that effect. When disputes arise as to what constitutes inappropriate Internet use, judges will be called upon for a resolution. If judges can be trusted to decide

264. Watson, supra note 180, at 97.
265. Id.
266. Id.
267. Id.
268. Id.
269. Watson, supra note 180, at 97-98.
270. Id. at 95.
271. Id. EPIC claims that the NEMA "may in fact increase the amount of overt surveillance, as companies under directions from their attorneys, write very broad policies outlining a wide range of possible surveillance activities that may not have previously occurred." Id.
inappropriate Internet use as applied to litigants, they can be trusted to
decide the issue as applied to themselves.

On its surface, the judicial debate over whether to monitor federal
designs' Internet use of workplace computers appears to be simplistic. A
closer examination, however, reveals the various competing interests
that need to be considered when implementing such a policy. The
Adopted Policy should not be implemented on a permanent basis
because of its failure to adequately incorporate the principles of judicial
independence, judicial accountability and judicial security. These three
traits distinguish the employer-employee relationship within the
judiciary from existing models of employee management.

The competing principles of independence and accountability have
led this controversial issue to become a current debate in the judiciary.

Any policy that impinges upon the independence of the judiciary must
be proportional to the harm redressed. Such proportionality cannot be
achieved by a ready solution. Continuous deliberation and consultation
are necessary to devise an Internet use policy that adequately balances
judges' concerns of privacy with society's concerns of judicial
efficiency.

Hardeep Kaur Josan and Sapna K. Shah

With gratitude and appreciation, I would like to acknowledge the following individuals:
my family, for their unyielding love, support and encouragement; M.J., for always listening;
Professor Roy D. Simon, for the opportunity to work under his guidance and advice; members of
the Journal, for their time and effort in editing this note; and Sapna, for her intellect, dedication and
hard work.

This note is dedicated to my parents, Kanu and Meena Shah, for their endless love,
continued support and guidance. They have encouraged me to excel academically and personally.
I extend my gratitude to my sister, Mamta Shah, who, throughout my life has been my strength, my
mentor and my role model. She has instilled in me the value of educational discipline and has taught
me that great power lies in knowledge, and it is to her that I owe my commitment to academia.
I extend my appreciation to Professor Roy D. Simon for his time and advice in the development of
this note. I am grateful to the editors and staff of the Journal for their insight and hard work. Finally,
I would like to thank Hardeep for her friendship, dedication and commitment to this note.