PILLSBURY WINTHROP LLP
ROBERT MITTELSTAEDT # 060359
JENNIFER STARKS # 215130
50 Fremont Street, 14th Floor
Post Office Box 7880
San Francisco, CA 94120-7880
Telephone: (415) 983-1000
Facsimile: (415) 983-1200

Attorneys for Plaintiffs
FRANK CLEMENT
[See Page 2 for additional
counsel representations]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

FRANK CLEMENT Plaintiff, vs. CALIFORNIA DEPARTMENT OF CORRECTIONS, et al., Defendants.	No. C 00-1860 CW **DECLARATION OF MIKE GODWIN IN OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT** Date: August 9, 2002 Time: 10 a.m. Before: Hon. Claudia Wilken

ADDITIONAL COUNSEL FOR PLAINTIFFS

Ann Brick #65296
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF NORTHERN CALIFORNIA
1663 Mission Street, Suite 460
San Francisco, CA 94103
Telephone: (415) 621-2493
Fax: (415) 255-8437

Donald Specter # 083925
Heather Mackay # 161434
PRISON LAW OFFICE
General Delivery
San Quentin, CA 94964
Telephone: (415) 457-9144
Fax: (415) 457-9151

I, Mike Godwin, declare the following:

1. I am currently a policy fellow at the Center for Democracy and Technology in Washington, D.C. I have held this position for two years. I submit this Declaration in support of plaintiff Frank Clement's Opposition to Defendants' Motion for Summary Judgment. Unless otherwise indicated, if called upon to do so, I could competently testify of my own personal knowledge to the facts set forth herein.

2. I have been working as an Internet law and policy expert in public-interest organizations 12 years. As a nationally recognized expert in this field, I am familiar with the legal and other issues deriving from the development of "cyberspace," including traceability of email and the risks associated with sending information over the Internet.

3. The Center for Democracy and Technology ("CDT") is a non-profit public policy organization that promotes the development of democratic values on electronic networks and protects the individual rights of those who interact with organizations, the government and other individuals over the Internet.

4. Prior to taking the position at CDT, I served as first Staff Counsel for Electronic Frontier Foundation where I worked on legal issues that arise by virtue of electronic networks. In 1998, I published my first book, Cyber Rights: Defending Free Speech in the Digital Age, Chapter Six of which deals expressly with questions of privacy and anonymity in cyberspace, and I regularly write articles on the interplay between individual rights and the Internet for IP Worldwide, American Lawyer, Internet World, Wired, HotWired, Time, Reason and Playboy. In 1991-92, I chaired a committee of the Massachusetts Computer Crime Commission,

where I researched issues pertaining to computer crime and co-authored the final report to the Governor concerning a computer crime statute. The recommendations in that report were subsequently passed into law by the legislature of the Commonwealth of Massachusetts.

5. Over the past ten years, the use of the Internet has skyrocketed. The growth of Internet-based companies as well as the number of services and information available online is phenomenal. Many businesses, governmental agencies and other organizations conduct their activities and provide information to the public primarily over the Internet. One consequence of this growth is that email has virtually replaced paper mail as the primary method of communication in the business world. Similarly, for many individuals email has become the preferred means of non-business communication. Email allows almost immediate communication without the delays and expense of using the U.S. mail or private carriers such as Federal Express.

6. It is increasingly the case that, if an individual wants to order a service, request information, peruse libraries, take classes, research an obscure subject, verify breaking news, obtain recent legislation, write to a congressman, he or she may facilitate all or part of any of those transactions through email, often but not always in conjunction with services on the World Wide Web, which, like email, is a service that is provided over the Internet.

7. In my view, because of the convenience and cost-effectiveness associated with communicating over the Internet, it will be increasingly difficult to obtain information, make requests, and conduct other lawful and necessary transactions via paper mail.

8. As our society undergoes the transition from one type of "mailed" communication to another -- from paper mail to email -- many officials and authorities become nervous. Everybody has grown up understanding how paper mail works, but email -- especially to older individuals -- may seem new, frightening, and incomprehensible. My experience has been that many individuals, including otherwise intelligent government officials and policymakers, reflexively view the Internet, email, and related technological advances as inherently more threatening. This gives rise, quite often, to negative generalizations about email, the Web, or the Internet as a whole that are without foundation. One of the most common false generalizations I have encountered is the generalization that email is inherently more anonymous and untraceable than traditional paper mail is. Once one has studied the question of how email works, it becomes clear that, as a practical matter, email is generally and routinely more traceable than paper mail. It is no surprise, given this fact, that Federal Bureau of Investigation agents investigating the terrorist attacks of September 11 found it relatively easy to quickly construct an evidentiary trail based in part on the suspects' email. It is also no surprise that the perpetrator of the anthrax-spore attacks in various public officials and public figures in New York City and Washington, D.C., has been able to stymie investigators for months, even though the delivery system for his attacks was based on supposedly safe and traceable traditional paper mail.

9. In general, e-mail leaves a trail -- often a complete trail between originator and recipient, and always a partial trail. Unlike paper mail, email commonly carries along with it a record of each computer on the Internet it passed through on the way to its recipient. Paper mail, in contrast, does not carry with it a record of every city or state it passes

through in transit. Moreover, while any child old enough to write a letter knows intuitively that one can do much to thwart the tracing of the letter simply by omitting to put a truthful return address on the envelope and mailing it from a public mailbox, it requires effort and knowledge for the sender of email to remove all identifying information from the email message, or to partially obscure the trail generated by the e-mail in transit. In my experience, relatively few of the millions of individuals who now use mail know (or care) enough to effectively obscure the evidence of its originator.

10. Typically, an originating email address is included in the header of the message. Often, these email addresses are based on a person's name. Like the return address or signature at the end of a letter sent by ordinary mail, the sender usually chooses the name he will use in his email address.

11. Most email programs also allow the user to view the path that the email followed as it traveled to the destination address. For example, the email program Eudora, which runs both on Windows computers and on Macintosh computers, allows any email recipient to view the path of an email -- contained in its "header" information -- simply by clicking on a button. Other email programs have similar features.

12. In addition, all Internet Service Providers ("ISPs") and email companies, including AOL, Microsoft Hotmail, Pacific Bell and Yahoo, assign an Internet Protocol ("IP") address to each user for a particular period of time. For example, AOL will be allotted a certain group of IP addresses to assign its users. When a user sends an email, the assigned IP address is imbedded in the "header" information of the email message.

Most casual users of email do not know that this information is readily available in the email header.

13. The IP address allows the receiver of the email message to identify what service provider acted as a host for the sender's message. The receiver of the message can then contact the ISP and subpoena the identity of the sender based on the IP address and the time and date that the message was sent. The ISP can review its records and determine which subscriber was using that particular IP address at a given date and time. (By comparison, the U.S. Postal Service cannot commonly or routinely tell us who is using a particular public mailbox at a given date or time.) The ISP knows that the information provided by the sender is accurate because that ISP bills the sender/ subscriber each month using the name and address provided by the sender.

14. The existence of an IP address distinguishes email from regular mail: while an individual who wants to conceal his identity in an email message must have some minimum level of sophistication to remove the IP address, the sender of a letter can easily exclude all identifying information from the envelope by using a false return address, using water to moisten the envelope flap and stamp, and mailing the letter from a distant post office or from a post office that has a very heavy volume of mail. By way of contrast, in order to hide one's identity using email one must research the use of anonymous-remailer services, and one must find a service that can be trusted to be "truly anonymous" -- that is, unable itself to recover information about the originator of a message. (Many so-called anonymous remailers retain originating information that can be recovered by investigating agents with an appropriate warrant or subpoena. This was the

case with the first anonymous remailer, known as anon.penet.fi, to become famous. When its operator, Johan Helsingius, a Finnish national, was presented with a court order for the true identities of those using his service, he was able to provide that information. In 1996, Helsingius shut down his service rather than be subjected to future process.)

15. In general, hiding one's identity with email requires an affirmative act with some specialized knowledge. Regular mail does not. Moreover, in my experience, most people do not attempt to disguise their identity when they are sending emails. In fact, the majority of the population is unaware of how much information they communicate about themselves simply by virtue of sending the email message.

16. It is true that senders can use a "remailer" to anonymize their emails. These remailers are often used by whistleblowers and other undercover sources who need to communicate information anonymously. However, all remailers whose services I have reviewed include a disclaimer at the top of the email stating, "This message did not originate at this address." I believe remailer operators insist on including such disclaimers so as to avoid potential legal liability in the event that someone uses their services criminally or fraudulently. In any case, a remailer is not the type of service that a person would use when he wants to conceal the fact that he is attempting to conceal his identity.

17. There are other ways to obscure or conceal originating information in email, including a practice that among Internet experts is known as "spoofing" email (that is, making the e-mail appear to come from someone other than who it is coming from). But these methods are themselves comparatively obscure. Individuals who are not Internet or

software experts will generally find it difficult to engage in any of these practices using ordinary email programs.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 14th day of June, 2002, at Washington, D.C.

Mike Godwin