

ON PUBLIC POLICY: CLARIFYING THE FEDERAL ROLE IN ENSURING CYBERSECURITY

Danielle Mihram, Ph. D.
Director, Center for Excellence in Teaching
University of Southern California
LVL-301B [MC #2571]
Los Angeles, CA 90089-2571
213 740 3783
dmihram@usc.edu

G. Arthur Mihram, Ph. D.
P.O. Box No. 1188
Princeton, N.J. 08542-1188
USA

ABSTRACT

We review and update the literature of tele-communications policy, particularly with regard to the calls [e.g.: 1) Kwok, CACM 46: 98-101, X.03; and 2) Greenemeier, INFORMATION WEEK, 24.I.05] for a governmental role in ‘cybersecurity’. We indicate the procedure by which tele-communications can be securely transmitted, yet in a manner alleviating concerns about privacy. Our proposal for a ‘National Electronic Postal Service’ would not just fulfill Congress’s duty to provide, in our Age of Tele-Communications (as opposed to the earlier Age of Written/Printed Communications), for (electronic) post-offices and (electronic) post-roads, as per the *CONSTITUTION OF THE UNITED STATES OF AMERICA*. An essential feature of this national electronic postal service would be its issuing securely (using electronic/digital watermarking) a governmentally-issued electronic postmark, one (when properly implemented) which would provide as well a mechanism for copyright-protection (another Constitutionally-mandated duty of Congress).

INTRODUCTION

We update our earlier calls for the establishment of a governmentally-operated ‘National Electronic Postal Service’ [Mihram and Mihram, 1999; 2000a; 2000b; 2001, e.g.]. The first of these here cited, according to feedback from readers, seems to be the most readable text; the subsequent papers added the conclusions of other authors, conclusions indicating an increasing awareness of the need for some form of governmental engagement in tele-communications, especially in the computer-connected tele-communications which are increasingly being referred to as “cyber-space”.

Our call herein is rather the same as that of our earlier papers: Congress itself possesses a Constitutional mandate to provide not only for ‘post-offices and post-roads’ but also for copyright protection, both still rather in need of updating now that we have moved historically from our earlier Age of Written/Printed Communications to our current Age of Tele-communications.

We shall therefore proceed here by rather curtly outlining our earlier arguments for “tele-cybernetics” [= ‘scientific politics in our Age of Tele-communications’]. We then note even more recent publications which call attention to the need for a governmental (i.e., political) role in tele-communications.

We then summarise our conclusions in the third ensuing Section.

TELE-CYBERNETICS

We derived etymologically this term (Mihram, 1975), as defined above, by calling attention to: (A) electrical engineer N. Wiener’s rather non-academic claim to have coined the term “cybernetics” as “control and communication in the animal and the machine”; yet, (B) the electrical scientist, Ampère, had in the early nineteenth century, when classifying human knowledge, pointed to Plato and concluded that ‘cybernétique’ means ‘the art of statesmanship: knowing not just what can be done; instead what must be done [in any particular political decision].’

The solution to the political aspects of the implementation of tele-communications and its policies requires, then, ‘tele-cybernetics’. The historical record reveals why the government of the republic requires the establishment of a

‘National Electronic Postal Service’’: (1) *THE CONSTITUTION OF THE UNITED STATES OF AMERICA*, the authors of which recognized that such a governmentally-operated postal service would assist in fulfilling one of the five (or six) reasons for having government: viz., to provide domestic tranquility; and, (2) the earlier establishment (17th Century France) of national postal services, founded originally by Cardinal Richelieu, a character in A. Dumas’s subsequent historical novel, *THE THREE MUSKETEERS*, the story therein relating the strife (i.e., the resulting domestic intranquility) resulting from “unregulated and multiple carriers” operating on “insecure roadways”.

THE NATIONAL ELECTRONIC POSTAL SERVICE

We continue to call for the establishment of a governmentally-operated (and –secured) national electronic postal service. Though we do not view this service as exclusionary, we recall others’ earlier observation that competing telecommunications commercial services do not possess the characteristic of having only its present ‘customer’s’ interest continually in mind (Mihram and Mihram, 1999).

This National Electronic Postal Service’s primary feature of importance is its issuance of a governmentally-secured “electronic postmark”, one which provides—like postally-despatched envelopes—“content-markers”, to include indication of contents with copyright-registration, and markings indicating the ‘level’ of pornography, violence, language, and drug-use depiction [P,V,L,D], ranging from, say, [0,0,0,0] to [9,9,9,9].

Recently, calls have arisen for more and more governmental participation in tele-communicaitons; e.g., Kwok (2003) notes that, in order to secure the use of ‘digital watermarking’ in electronic copyright protection, government should be involved; Greenemeier (2005) notes that a federal role in ensuring cybersecurity requires specification; and, right to the point of this paper, Stross (2005) suggests in the *NY TIMES* that the annoying ‘spam’ [= unsolicited commercial e-mail] might well be controlled by recalling the first postal stamp (England’s ‘Penny Black’], then implementing this electronically.

Our call for the National Electronic Postal Service appears to be increasingly supported. A National Electronic Postal Service, with its electronic postmark, would likely have to be supported by a service fee (like one’s subscription to an E-mail/Web service currently), either a periodic (monthly, annual) tax and/or a suer fee (a rate schedule for each electronic transmittal/delivery).

A structure of postal laws and regulations shall need be established and enforced. For example, electronic postmarks issued via digital watermarking can assist greatly in providing authentication of a claimed sender and subsequent authorization for being granted access to (and retrieving from) a distant computer-controlled electronic data file.

We propose also procedures for avoiding both censorship and the concerns for privacy, particularly as the latter may deal with access to electronic data files of a decidedly personal or corporate nature.

Privacy

As for the latter (concerns re privacy), we propose that it be legislatively mandated that every computer giving access to any file of such ‘sensitive’ or personal data maintain a registry-log of the electronic postmarks (with requisite biometrics) requesting access. The log would be required not only to record exactly which data elements are being requested and then which have been released but also to note the exact “electronic postal address (biometrics included)” making this request and then the address receiving the requested material.” Legislation will need to enforce restrictions on any re-transmission of such supplied information, perhaps via properly implemented ‘electronic postmarks’ which report every such re-transmission to the ‘log’ of the originating data station.

Periodically, each person whose sensitive/corporate information is in such accessible files should receive (quarterly, annually?) a report of each of these transactions, whether merely attempted or granted.

Perhaps the implementation of the digital copyright mechanism would facilitate this procedure, though some mechanism for restraining or reporting the downloading of materials for printing would need be established as well. We return to this matter of copyright protection in the next sub-section.

Another matter dealing with privacy arises in the context of law enforcement and/or prosecutorial access to electronic records of such personal/corporate materials. Clearly, such officials must be granted access—but strictly under court order—to such files, yet the periodic reporting to any investigated party would not need be revealed (except under court order, as guide the revelation of evidence between prosecutorial and defense attorneys).

Copyright protection

We have called earlier for the use of digital watermarking at the very time of a document/publication/video/voice-recording's electronic copyright-registration, so that only two original electronic copies would possess the "electronic copyright seal": that returned to the copyright applicant (publisher/producer); and, that one, if purchased by the [Electronic] Library of Congress, of this archival institution.

Censorship

Clearly, criminal enforcement of electronic privacy and electronic copyright via legislation shall be necessary. Similarly, with the use of (requisite) content-markers for the levels of [P,V,L,D] = [Pornography; Gratuitous Violence; Obscene Language; and, Drug-use Depiction] within the electronic postmark, one needs to avoid concerns re governmental 'censorship'. We are not here proposing that there be a governmental (electronic postal service's) refusal to transmit/deliver objectionable materials, unless, of course, an intended recipient has placed the particular electronic sender on his "No-call" list with the "Electronic Postmaster". We are merely noting that there must be a governmental responsibility to require (as with the postal service) that content-markers, under penalty of law, be required, even in the electronic copyright-registration procedure. It is then left to private firms (video reviewers, like book reviewers) or religious organizations either to confirm any electronic publisher's [P,V,L,D]-rating or to provide their own. Parents and teachers may subscribe to one or more of these rating services and thereby restrain their local computer from accepting any download of objectionable material.

Electronic Evidence

Another of the five or six reasons [cf. Preface, *THE CONSTITUTION OF THE UNITED STATES OF AMERICA*] for establishing government (republic) is 'to establish justice'. Legislation requiring that commercial and/or governmental electronic databases be properly maintained (Foster, 2005)—so as to enhance, rather than inhibit, the collection of data requisite for prosecuting suspected criminal behaviour—can also be improved by the implementation of date-marking technologies such as the digital-watermarking, even increasing the reliability by means of commercial access to the National Electronic Postal Service so as to secure a certifiable 'electronic date/time stamp' for each element in a commercial company's data files.

We note the matter of protecting the privacy of personal/corporate matters, whenever these are involved in investigative or prosecutorial activities (See the third preceding sub-section.).

CONCLUSIONS

Our earlier call for a National Electronic Postal Service, with its governmentally-issued electronic postmark (one requiring content-markers and, as necessary, biometric identifying information), seems to be warranted. Numerous publications now are calling for 'electronic postal stamps' or for 'a governmental role' in copyright protection or for ensuring cybersecurity (the joint issue of authentication and authorization). The original recognitions of the need for a "national [electronic] postal service (viz., *THE THREE MUSKETEERS*'s 17th-Century Cardinal Richelieu as the Founder/Father of the postal service; and, *THE CONSTITUTION OF THE UNITED STATES OF AMERICA* (1787)] is apparent, else we re-discover (the quite avoidable) domestic intranquility in our Age of Tele-communications.

REFERENCES

Foster, A. L., "Yale Law Students Urge Court to Support Requests for Electronic Evidence," *CHRONICLE OF HIGHER EDUCATION*, 4 March 2005: A34.

Greenemeier, L., "Federal Role in Ensuring Cybersecurity Isn't Clear," *INFORMATION WEEK*, 24 Jan 2005.

Kwok, S. H., *COMMUN ASSOC COMPUT MACHIN* 46: 98-101, Oct 2003.

Mihram, G. Arthur, *AN EPISTLE TO DR. BENJAMIN FRANKLIN*, NY: Exposition-University Press, 1975(1974).

Mihram, G. Arthur and Danielle Mihram, "Tele-cybernetics: Guidance Toward Information Dominance and Assurance," *FEDERAL DATABASE COLLOQUIUM*, pp. 335-350 (Washington, DC: A.F.C.E.A.), 1999.

Mihram, G. Arthur and Danielle Mihram, "Resolving Two Congressional Duties: Electronic Copyright and the Electronic Post-offices—and—Post-roads," *PROC, COMPUTERS IN LIBRARIES*, pp. 195-204, 2000a.

Mihram, G. Arthur and Danielle Mihram, "Tele-cybernetics: On Some necessary Governmental Roles in the Internet and the Web," *WEBNET 2000*, electronic proceedings w/o pagination, 2000b. See: <<http://www.informatik.uni-trier.de/~ley/db/conf/webnet/webnet2000.html#MihramM00>>

Mihram, G. Arthur and Danielle Mihram, "Tele-cybernetics: Some Congressional Roles in the Internet, the Web, and Desktop Publishing," *PROC, TRENTON COMPUTER FESTIVAL*, pp. 23-33 [See also the subsequent proceedings of 2002 and 2003], NY: I.E.E.E., 2001.

Stross, R., "How to Stop Junk E-mail: Charge for the Stamp," *NY TIMES*, 13 February 2005, p. Bus 5, 2005.

BIOGRAPHICAL SKETCHES

Dr. Danielle Mihram, currently Director of the Center for Excellence in Teaching, a position on the staff of the Provost of the University of Southern California, has co-authored a number of papers dealing with tele-communications policy. Her biographical sketch has appeared in Marquis's *WHO'S WHO OF AMERICAN WOMEN*.

Dr. G. Arthur Mihram's biographical sketch appears in Marquis's *WHO'S WHO IN AMERICA* and *WHO'S WHO IN THE WORLD* (2005).