Writing is Public on the Internet (And That's Good)

Catherine F. Smith

Relative to the Internet, what does 'public' mean? Narrow meanings inherited from the binary, public vs. private, create tension or contradiction in writers' and teachers' attitudes toward the network. If we set the traditional binary aside, what might 'public' mean for network writing? Expanded meanings include 'common goods,' or private resources used for public benefit. The past history of public communication also supports a reconception of the Internet as a resource for public life.

Introduction: A Problem Context

Students are sometimes reluctant to publish their coursework on the Internet while teachers are reluctant to force students into unwanted public disclosure. Two such teachers who assigned personal narratives to be posted in a class World Wide Web site then found students to be worried about family members reading their accounts. Those teachers recently remarked that "we are left unsure how to meld the public space of the Internet and the narratives of [students'] private lives."

There are, of course, technical solutions such as password-protection for coursework to block readers lacking the proper password. But I want to address the attitudinal problem. I want to develop a philosophy of writing that is network-sensitive and public-affirmative. My effort pivots on rethinking 'the public space of the Internet.' We (writers and writing teachers) need to reconsider the tacit and explicit ideas of 'public' communication that we bring to the network.

WORKS AND DAYS 33/34,35/36 Vol.17&18, 1999-00

Rethinking the Problem

The traditional binary, public versus private, does not help much. In fact, it inhibits fresh thought because it assumes opposition when the real problem in its present form is the blurring of boundaries between public and private. Similarly, the real opportunities for fresh thinking are situated where public and private presently intersect. So, if we abandon binary thinking, we clear the way for fresh conception. In brief remarks here, I will sketch an enriched idea of 'public' specific to the Internet and oriented to writing classroom needs. I limit my remarks to the World Wide Web (WWW), which has become the common classroom interface for the network.

I want a pedagogy of writing publicly that:

> *fosters positive attitudes toward WWW writing and addresses discomforts of writing in that medium
> *builds rhetorical awareness of an audience of nobody, which means anybody—any person or network process—that might interact with WWW text, and
> *develops literacies of presence, or abilities to live and to tell stories about it mindful of the presence of others, each different.

Definitions of 'Public'

Several disciplinary approaches to defining 'public' are useful for my purpose. In philosophy and ethics, Jurgen Habermas's idea of communicative action and Hannah Arendt's concept of the human condition frame a 'public' based on normative commonality. Criticism has identified limitations in their articulation, and offered a useful expansion to conceive diverse 'publics' co-occurring in shared space (Calhoun). Also suggestive, in sociology, is Erving Goffman's multi-dimensional work on social orders or 'little societies' created by interaction (*Behavior*, *Frame Analysis*, and "Interaction Order"). In anthropology crossed with pragmatic linguistics, Penelope Brown and Stephen Levinson's work on 'face' management might be fruitfully applied to Internet 'presence.'

However, my students often have not read these works when they come to my writing courses. My students' preconceptions of 'public' writing are most likely based in their other writing experiences and in other instruction. Recently, to learn what tacit models of 'public' might be traveling with my students into my courses,

I telephoned faculty colleagues in law, public communication law, public policy studies, and cultural anthropology who teach the juniors and seniors likely to enroll in my advanced electives in WWW writing. I asked these faculty colleagues two questions: How do you define 'public?' If a student asked you how the Internet is 'public,' what would you say?

Individually, their answers can be paraphrased as follows:

> -Public law is regulative for all; private law is contractual or tort (e.g., injury, liability) for individuals, although the distinctions have eroded and their applicability to the Internet is unclear (law).
> -Public means everything and everybody, but just because something's on the Internet does not mean it is public (legal research).
> -Public means 'addressed to more than one person or to a mass of people;' information can also be 'made public,' after which regulation applies; the Internet intensifies legal questions pertaining to all media and brings its own peculiar questions, e.g. 'are service providers publishers?' (journalism).
> -Public is synonymous with government or the administration of public life; the Internet is not public in that sense (policy studies).
> -Public is defined by users; behavior may be either public or private according to convention or agreement (anthropology).

Collectively, those colleagues outlined a set of ambiguities affecting views of the Internet as a public medium. Probably, any other random selection of colleagues would only add more ambiguities. No wonder students are ambivalent about using the network.

Therefore, toward a use-based definition of networked 'public' I offer this conception: 'public' is a quality of an action or an entity. 'Public' thus becomes an adjective or adverb, not a noun. It is an attribute assigned by an observer or user according to a set of values.

That might be good, or bad.

The bad is evident in the current computer use policy for the institution where I teach, Syracuse University. (The policy is attached, here. You might want to look at your own institution's policy, too.) If you skim our policy, I think you will see a grab bag of rules for several behaviors: social interaction, contractual rela-

tions, and use of a shared utility. Syracuse tries to address fairness, equality and equity, and liability in one policy. In my remarks here, I offer my institution's policy illustratively. It encapsulates the ambiguities, contradictions, and ambivalence with which an educational institution views the Internet. In class, I draw students' attention to the policy without extensive comment. Students need to know that this policy is part of the university's code of conduct, and that violations may lead to disciplinary action possibly affecting their progress or their standing.

A Better Way: Classroom Example

However, I do not agree with my institution's policy. I believe it generates fear and discourages educational uses of the network. Without challenging the mixed-bag policy directly, I make a pedagogical counter-move. I try to generate students' positive wish to write on the network *because* it is public. I suggest that the public character of the medium is one of its most interesting features because that feature demands that users consciously relate online and off-line life.

For example, in my professional and technical communication courses using the WWW, this demand arises because students design and develop Web sites for clients. Because I do not restrict them, clients might include campus groups, off-campus groups, or businesses (family-owned or student-owned). Thus, students might potentially violate provisions of the university computer use policy against commercial use, prohibited behavior, or use that overloads the system. In several years of such courses, no student has actually gotten into trouble. However, such policies tacitly constrain teaching and learning. I suggest that teachers might respond by strategically making students aware of current policy, and by making better policy in the classroom. (Note: Having a course policy may also be a good defense if the need arises. Instructors' policies can mitigate disciplinary proceedings; such policy for educational purposes may help a student who does get into institutional trouble.)

Specifically, I suggest that we add a policy component to our pedagogy for WWW writing courses. Start a conversation with students early, before they take up assignments, about resources for and conditions of work in your course. Teach the need for policy and offer practice in articulating a classroom policy. With client Web sites, my students and I recognized a need for a policy having to do with graphics. These were the issues: both students and

clients wanted lots of graphics (a condition). The time required to download images significantly affects a Web site's usability (a condition pointing to a resource issue—time). Affordability of Web services was a problem for some clients or for their own customers (a condition pointing to another resource issue—money). Consequently, we worked out a policy mandating maximum image size in order to support low-cost access. Educationally, this policy-making process accounted for my students' interest (creative design), their clients' interest (functional, affordable web sites), the local community's interest (avoiding slowdowns on the campus network), and the instructor's interest (user-based design). Our classroom policy addressed the intent (if not the letter) of institutional policy-making, and we did it as an educational exercise (Smith).

Conclusion: Why Writing Publicly Is Good

Earlier, I asked that we set aside traditional ideas of 'public' in order to let a richer idea emerge. Arendt's ethical perspective informs the enriched idea that I advocate here. For Arendt, 'public' signifies two qualities: can be seen and heard by all, each differently, and occurs in the space of human interest or "something which inter-est, literally *is between*" (182). Classroom policy-making offers practical experience in exploring that territory on the Internet.

To frame the idea further, I offer one historical analog. It is not about classrooms, but it is relevant nonetheless. In the 1780s and 90s when native Indian nations, European nations, and the new United States nation negotiated co-existence on the same North American continent, they negotiated in deliberately public ways. For deliberation to be seen and heard by all was essential to a treaty's authority. Public negotiation made possible a record of agreements preserved in memory or in writing to sustain proper enforcement beyond the immediate present. Thus, a condition of authority was public disclosure, or action taken in public view.

It is this quality of stabilizing and sustaining human life through public discourse that I wish to assign to Internet writing. Informed by past historical valuations of communicating publicly, disclosure might be re-valued so that network writers and teachers who presently see it as negative might come to see it, instead, as affirmative. Disclosure might be a condition that authorizes the existence of multiple versions of reality, each different, and makes them accessible for the common good.

Works Cited

Arendt, Hannah. *The Human Condition*. 1958. Chicago: U Chicago P, 1989.

Brown, Penelope and Stephen C. Levinson. *Politeness: Some Universals in Language Usage*. Cambridge: Cambridge UP, 1987.

Calhoun, Craig. *Habermas and the Public Sphere*. Cambridge, Massachusetts: MIT P, 1992.

Goffman, Erving. *Behavior in Public Places: Notes on the Social Organizations of Gatherings*. London: Macmillan, 1963.

—-. *Frame Analysis: An Essay on the Organization of Experience*. New York: Harper's, 1974.

—-. "The Interaction Order." *American Sociological Review* 48 (1983): 1-17.

Habermas, Jurgen. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Cambridge, Massachusetts: MIT P, 1989.

Smith, C. "Nobody, Which Means Anybody: Audience on the Web." *Weaving a Virtual Web: Practical Approaches to Teaching with Technology*. Ed. Sibylle Gruber. Champagne-Urbana, Illinois: NCTE P, 1999.

Syracuse University Computing Policy (January 1999). 21 Feb. 2000. <http://cms.syr.edu/policy/>. Cited with permission of Computing and Media Services, Syracuse University, Syracuse, New York.

Appendix

Syracuse University
Computing and Media Services
(http://cms.syr.edu/policy/computepolicy.html)

SU Computing and Electronic Communications Policy

This policy governs the use of computers, networks, and related services on the Syracuse University campus. Users of these resources are responsible for reading and understanding this policy. Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such access is a privilege and requires that individual users act responsibly. Users must respect the rights of others, respect the integrity of the computers, networks, and related

services, and observe all relevant laws, regulations, contractual obligations, and University policies and procedures.

The Syracuse University Computer System

The Syracuse University Computer System includes: computers, communications networks, computer accounts, web pages, network access, central computing and telecommunications facilities, and related services. The Computer System at Syracuse University is maintained by Computing & Media Services ("CMS"), located at 120 Hinds Hall.

Access to and use of the University's Computer System is a privilege granted to currently enrolled Syracuse University students, faculty, and staff. All users of the Computer System must act responsibly and maintain the integrity of the Computer System. The University reserves the right to deny, limit, revoke, or extend computing privileges and access to the Computer System in its discretion. In addition, alleged violations of this policy or violation of other University policies in the course of using the Computer System may result in an immediate loss of computing privileges and may also result in the referral of the matter to the University Judicial System or other appropriate authority.

All messages, data files and programs stored in or transmitted via the Computer System ("Electronic Communications") are Syracuse University records. The University reserves the right to access and disclose all messages, data files and programs sent over or stored in its Computer System for any purpose. It is the responsibility of all users of the Computer System to notify CMS about violations of laws and University policies in connection with the use of the Computer System, as well as about potential loopholes in the security of the Computer System. The user community is expected to cooperate with CMS in its operation of the Computer System, as well as in the investigation of Computer System misuse or abuse. Any concerns, complaints, or reports of misconduct with regard to the Computer System should be reported to the Director of Client Services at 443-3631.

Computer Accounts. Computer accounts are issued to University faculty, staff, and students, and other individuals at the discretion of CMS, for University purposes. These accounts must not be used for commercial purposes. Every computer account issued by the University is the responsibility of the person in whose name it is issued. That individual must keep the account secure from unauthorized access by keeping the password secret, by

changing the password often, and by reporting to CMS when anyone else is using the account without permission. Passwords are intended to help prevent unauthorized access and may not be shared. The contents of all accounts are subject to access and disclosure by the University as set forth in this policy.

Improper Use of the Computer System. Improper use of the Computer System is prohibited. The following are examples of improper use of the Computer System:

> **Prohibited Behavior:** Storing, transmitting or printing any of the following types of Electronic Communications on the Computer System is prohibited: material that infringes upon the rights of another person; material that is obscene; material that consists of any advertisements for commercial enterprises; material or behaviors that violate the Syracuse University Code of Student Conduct or other University policies; or, material that may injure someone else and/or lead to a lawsuit or criminal charges.
>
> **Harassment:** Harassing others by sending annoying, abusive, profane, threatening, defamatory or offensive messages is prohibited. Some examples include: obscene, threatening, or repeated unnecessary messages; sexually, ethnically, racially, or religiously offensive messages; continuing to send messages after a request to stop; and procedures that hinder a computer session.
>
> **Destruction, Sabotage:** Intentionally destroying anything stored on the Computer System, including anything stored in primary or random access memory is prohibited. Deliberately performing any act that will seriously impact the operation of the Computer System. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer or peripheral.
>
> **Evasive Techniques:** Attempts to avoid detection of improper or illegal behavior by encrypting electronic messages and computer files are prohibited.
>
> **Unauthorized Use/Access:** Using the Computer System to gain or attempt to gain unauthorized access to remote computers is prohibited. Other prohibited

behaviors include: actions that give simulated sign off messages, public announcements, or other fraudulent system responses; possessing or changing system control information (e.g., program status, protection codes, and accounting information), especially when used to defraud others, obtain passwords, gain access to and/or copy other user's electronic communications, or otherwise interfere with or destroy the work of other users.

E-Mail Forgery: Forging e-mail, including concealment of the sender's identity, is prohibited.

Theft/Unauthorized Use of Data: Data created and maintained by the University, or acquired from outside sources, are vital assets of the University and may be subject to a variety of use restrictions. Theft of or unauthorized access to data is prohibited.

Program Theft: Unless specifically authorized, copying computer program(s) from the Computer System is prohibited.

Viruses, etc.: Running or installing on the Computer System, or giving to another, a program that could result in the eventual damage to a file or the Computer System, and/or the reproduction of itself, is prohibited. This prohibition includes, but is not limited to, the classes of programs known as computer viruses, Trojan horses, and worms.

Security: Attempting to circumvent data protection schemes or uncover security loopholes is prohibited.

Wasting Resources: Performing acts that are wasteful of computing resources or that unfairly monopolize resources to the exclusion of others is prohibited. These acts include, but are not limited to: sending mass mailings or chain letters; creating unnecessary multiple jobs or processes; generating unnecessary or excessive output or printing; or, creating unnecessary network traffic.

Accessing User Accounts: Attempting to access or monitor another user's electronic communications is prohibited. Accessing, reading, copying, changing, disclosing, or deleting another user's messages, files or software without permission of the owner is prohibited.

Recreational Use: Recreational use of the Computer System that interferes with the ability of other users to complete their work is prohibited. In particular, if you are using a machine in a Public Computer Cluster for

> recreational purposes, and others are waiting to use a machine for academic purposes, you are expected to give up your seat.

Public Computer Clusters. Public Computer Clusters are part of the Computer System operated by CMS and are a shared University resource available on a first-come, first-served basis. A valid University or SUNY ESF (State University of New York Environmental Sciences and Forestry) ID card is required to use the Clusters. Food and beverages are prohibited in the Clusters. Clusters may be reserved for exclusive use by a class or group; schedules are posted on each Cluster's door and published electronically to various new groups every week. Some Clusters are provided by departments other than CMS; contact those departments for their additional usage guidelines.

Mail Distribution Lists. Mail Distribution Lists (often called LISTSERV lists) facilitate E-mail discussions on specified topics. Syracuse University faculty, staff, and students may request to sign up for list maintenance and membership, and have the discretion to control list content. List owners should not add subscribers to their list without the knowledge and consent of the subscriber to be added.

The University does not monitor the content of Mail Distribution List e-mail, except as otherwise provided in this policy, and is not responsible for the content of such messages. However, the University may terminate lists that consume excessive resources or are no longer relevant to the purposes of the University. In addition, the University may take action where lists violate this computing policy or other University policies. Posting of material unrelated to a list's usual content may be prohibited in the discretion of the list's owner. Posting unrelated material to multiple lists ('spamming') will be grounds for account revocation and other disciplinary action.

General e-mail announcements to the University community, such as HOTNEWS and system "Messages of the Day", are limited to those messages that concern University business and are deemed to be of the greatest interest to the most recipients.

Backup Copies. Data on the Computer System are subject to backup at the discretion of the University.

Deleting Electronic Communications. Users of the Computer System should be aware that electronic Communications are not necessarily erased from the Computer System when the user 'deletes' the file or message. Deleting an Electronic

Communication causes the Computer System to 'forget' where the message or file is stored on the Computer System. In addition, Electronic Communication may continue to be stored on a backup copy long after it is 'deleted' by the user. As a result, deleted messages often can be retrieved or recovered after they have been deleted.

Computer Law. Under Article 156 of the New York State Penal Code, criminal sanctions are imposed for offenses involving computers, software, and computer data. The offenses include unauthorized use of the computer, computer trespass, computer tampering, and unlawful duplication or possession of computer related material. Improper or unauthorized access to, or release or manipulation of, any student record in such form is included in such offenses.

All computers, software, data, business records, and student records of the University in any form, including electronic or paper, belong to the institution. Any person committing an offense with respect to them may be subject personally to criminal sanctions and other liability. Federal laws may also apply to some circumstances.

Copyright Infringement. The Copyright Laws of the United States prohibit unauthorized copying. Violators may be subject to criminal prosecution and/or be liable for monetary damages.

In general, you may not copy, download, install or use software on the Computer System without acquiring a license from the publisher. (For example, you may not copy it from a friend or other source.) Furthermore, you may not copy the University's software, unless such copying is specifically permitted by the license agreement.

The ability to download documents from the Internet, and to attach files to e-mail messages, increases the opportunity for and risk of copyright infringement. A user can be liable for the unauthorized copying and distribution of copyrighted material through the use of download programs and e-mail. Accordingly, you may not copy and/or distribute any materials of a third party (including software, database files, documentation, articles, graphics files, audio or video files) unless you have the written permission of the copyright holder to do so. Any questions regarding copying or downloading should be directed to CMS.

VII

Critical Reflections on Project UNLOC