ALTERNATIVELY AS SPEAKING

VOL. 5, NO. 2

IN THE SPOTLIGHT

Privacy and AAC

As our spotlight casts its glow on privacy, we see a complex subject. Privacy is a human right, a sign of respect from one person to another and a way to set financial, legal, physical, social and emotional boundaries. In this issue of *Alternatively Speaking* we will exam some of the privacy issues which augmented communicators may face.

Roots

Expectations about privacy and people with disabilities are changing. A slogan from South Africa that has caught on internationally with the disability rights movement is, "Nothing about me without me." This slogan reflects a commitment to ensuring that each person with a disability is involved to the maximum extent possible in decisions that affect him or her. A mere thirty years ago, decisions about social services, clinical services, education, employment and medical care of people with severe speech disabilities typically were made FOR augmented communicators not WITH augmented communicators. The training and experience of most professionals have not prepared them to establish personal or professional relationships with augmented communicators who say, "Nothing about me without me." Likewise, most community and family members do not have the social expectations and personal experiences to support augmented communicators who say, "Nothing about me without me."

INSIDE THIS ISSUE

As we encourage the world to catch up with "Nothing about me without me," some people with disabilities are adding, "and sometimes just me." Family members, helpers, clinicians, and educators may feel like they are suddenly being shut out. They may feel like they are not fully in control of their clients and family members. A goal of all augmented communicators should be to learn to take control of their own lives.

The old ways were wrong, but they are deeply embedded into our cultures. No one is going to feel completely comfortable with augmented communicators exercising their rights to privacy.

Conditions

Just having a severe speech disability creates conditions that discourage the usual kinds of privacy. The severely disabled child is protected and watched over out of legitimate concerns for safety. Group living situations can limit privacy. Professionals in charge of treatment or services may not realize they are intruding on a client's privacy, or they may find it inconvenient not to. Many

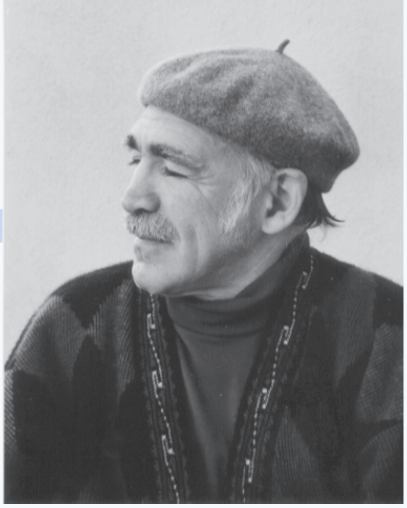
Continued on page 2

Message from the editor

During a visit to my doctor the other day, I was casually informed that he is swiftly moving toward a "paperless office." Records that now reside on paper in files at the doctor's office are rapidly being transferred to a computer hard disk in the same office. But this is only a temporary arrangement. Eventually, all the records, including mine, will be stored at a remote location on the Internet.

Electronic technology is changing and growing quickly. Our cultures and governments can't keep up. We know the consequences of reading someone else's diary or journal. We know what will happen if we get caught going through Dad's bureau drawers. We know to pretend we can't see in bedroom windows as we walk at night. But we have very little idea how to keep our personal electronic data safe. Whenever one of my children gets into something off-limits, I yell, "Put it up high," while my wife responds, "I want a safe." Neither "up high" nor a "safe" is a practical solution for electronic data.

The field of augmentative communication is not immune to this laissez-faire climate. As the footer on the ACOLUG listserv says, "Please remember that all messages posted to ACOLUG are public, and copies of them remain on-line as a permanent part of the ACOLUG archives." Clinicians have access to electronic technology that used to be available only to researchers. With automated data logging, researchers and clinicians can quickly collect and analyze communication data that used to require hours of tedious work. Clinical records can be emailed to anyone in a moment's notice. All this is possible, but will it benefit AAC consumers in the long run? The promise of electronic technology is so great that few are stopping to analyze the social, political, legal, psychological or moral ramifications.



ALTERNATIVELY SPEAKING (ISSN 1075-3982) is published quarterly by Augmentative Communication, Inc., 1 Surf Way, Suite 237, Monterey, CA 93940. Telephone: 831-649-3050. FAX: 831-646-5428.
One Year Subscriptions: By personal check U.S. & Canada=$35 U.S.; Overseas=$45 U.S.; Institutions: U.S. & Canada=$50 U.S.; Overseas=$60 U.S. Single Issues $13.
Special rates for consumers and full-time students.
Second-Class Postage Paid at Monterey, CA. POSTMASTER: Send address changes to ALTERNATIVELY SPEAKING, c/o Augmentative Communication, Inc. 1 Surf Way, Suite 237, Monterey, CA 93940-3451.

Editor: Michael B. Williams Technical Editor: Carole Krezman
Guest Authors: Jeff Higginbotham, Rick Hohn, Carole Krezman, Bob Segalman and Eda Wilson

Continued from page 1

of the accepted boundaries regarding privacy are crossed as a necessary part of personal care or physical therapy. It is difficult for people with disabilities to re-establish and maintain their boundries once these boundaries have been crossed.

Augmented communicators have been advocating for improvements in services, education, personal care and assistive technology. These improvements bring the perceived need to track treatment success, the desire to monitor treatment and care, a focus on outcomes and an emphasis on making the technology work. Augmented communicators have a cultural history of being abandoned without communication in human warehouses and "special" schools. They may have had personal experience offending someone whom they rely on for care or services. "No. Don't touch that. This is mine. Leave me alone," are not foremost in the minds of many augmented communicators. Not many augmented communicators are going to risk losing the assistance and support they have been struggling for in order to gain some privacy.

Control

It is very difficult to talk about privacy without mentioning control. The individual who sets and maintains rules or personal boundaries for his or her own privacy is exerting control. The agency, facility or institution that sets privacy standards for its employees who interact with

Continued on page 5

Securing Confidentiality in DynaVox and DynaMyte

by

Rick Hohn

Rights to privacy are guaranteed for everyone in free countries. Augmentative communicators are no exception.

After hearing that some people don't believe that privacy should be an issue in AAC, Bob Cunningham, Vice President of Research and Development for DynaVox Systems Inc. said, "I completely reject the notion that 'honest' augcomm users don't have anything to worry about. Everyone has a right to expect privacy."

There are a few ways that DynaVox and DynaMyte users can prevent other people from changing their systems' setup and can secure confidential information in their devices.

A password

The first method is through the Programming Lock and the Password feature. The Programming Lock option ring lets you 1) activate the password protection of the Setup Menu, 2) block the use of menu features that modify or delete information and 3) block the use of command buttons on pages or popups. This feature prevents anyone from changing how your device is set up unless the password is given. Although a password can be changed, it isn't easy to do, as it requires the knowledge of another password that is commonly unknown.

Hiding information

If you want to hide personal information written in document files, you can keep them out of sight by moving them into a separate folder or directory. Rename these files to folders that snoopers wouldn't suspect. These files can also be stored and hidden in additional, remote directories where nobody would think to look. You alone can find these files through a complex retrieval procedure.

Hidden backup

Another way to prevent someone from changing your system is to make a backup file that would be unnoticed by other people. To do so, make a backup file with another name—unsuspicious to anybody—like "child.bck". Then, move and hide your backup file in a remote directory. This process makes it almost impossible for anybody to find.

Secret numbers

In addition to hiding backup files, there is a way to secure personal information, such as credit card and social security numbers, on a dynamic display page. First, create a page of important information that can be disguised using a deceptive symbol button. In the label field, create a long sentence about anything. At the end of the sentence, insert the classified information. It won't appear on the button. To view this information yourself, go into the label field and then go to the end of the text. You will be able to see your hidden classified information. After designing this layout, make a link button on a page of the same color. The link button will blend into the page background so only you know where this link is.

Conclusion

All of these methods can make your DynaVox or DynaMyte device, and the information in it, safer and more secure. Be sure to keep notes separately on the file names, directories and any methods you use so that you won't forget them and lose access to your important information.

Problems and Solutions

By Jeff Higginbotham, Ph.D., an

For almost twenty years, my lab has collected and analyzed data produced by augmented speakers and their communication devices including key presses, button clicks, scanning transitions, timing data and words.

As part of the RERC on Communication Enhancement, we are working on ways to automatically collect and analyze information produced by AAC devices. This is called automated data logging or ADL. ADL may, one day, provide valuable information to improve the design of communication devices, assist with device selection and boost communication performance.

As researchers, we are aware that recording someone's communications provokes a number of issues concerning a speaker's right to privacy, communication control and freedom of speech. After making the decision to forge ahead with our automated data logging project, we began to work with clinicians, augmented communicators and manufacturers to build safeguards that ensure the ethical use of this type of technology. Below are some of the issues that we have grappled with and our solutions to these problems.

Access to stored information

AAC devices store various aspects of a speaker's communication performance in the form of text buffers, logfiles, user dictionaries and statistical information. Both buffers and logfiles store messages produced by the device that can be viewed at a later time by another person. There are several ways in which devices can be designed to protect the augmented speaker's privacy.

- AAC devices should be equipped with a CLEAR button that erases the screen as well as the buffer.
- Logfiles should be encrypted by default to prevent unintended viewing.
- Devices should have an indicator that shows when the device is recording to a logfile or storing information in a buffer.
- Device users should be able to easily start, terminate and erase any stored information.

Permission to collect

With advances in logging technology, AAC devices can record an augmented speaker's performance on a device over long periods of time across a wide variety of situations. Thus, to ensure that the augmented speaker understands the privacy issues of automated data logging, he or she should have the opportunity to provide informed consent. We recommend that in education, clinic and research settings augmented speakers and family members should be fully informed of the use and implications of any proposed data logging. Clinicians and researchers should have clear, specific questions that can be answered by collecting each kind of data, and they should request permission for each type of data collected. They also should be clear about the reasons for the duration and settings of data logging.

Clinicians, as well as researchers, should take precautions to insure that the reasons for collecting data are fully explained to and understood by the augmented communicator and the family. This may include providing information about the:

- kinds of information being sought. *(May we collect information relating to speed and accuracy and to vocabulary use? May we log the text from your communications?)*
- settings where data would be logged. *(May we record your communications in the classroom for the next two days?)*
- duration of recording. *(May we record your scanning transitions over the next two days?)*
- expectations of the augmented speaker during the clinical procedure. *(Please communicate as you normally would during the course of each day.)*
- how confidentiality will be maintained. *(Your conversations will never be shown to another person. May we write summary data into your clinical record?)*
- security and intended use and disposal of the data. (May I store all information on my computer

in Data Logging

AAC RERC partner

IN THE SPOTLIGHT

Continued from page 2

system? May we disseminate your data without any personally identifying information? May we keep your logfiles for one year?)

Permission to analyze

The augmented communicator should be able to control what aspects of his or her communications may be analyzed. It may help to know that valuable statistics can be obtained from encrypted logfiles without viewing actual communications. The clinician/researcher should have clear, specific questions he/she plans to answer before doing each type of analysis and should request permission before embarking on each type of data analysis. Finally, the clinician/researcher should specify how the results generated by an analysis will be used.

Other considerations

- Clinicians/researchers should assure augmented speakers and their families that the procedure is voluntary and that if they are not willing to participate in any aspect, or want to terminate participation at any point, they will not experience any negative consequences as a result.
- Augmented speakers should receive instructions for starting and stopping the logging process and for erasing logfiles that contain private information.
- The clinician/researcher should specify how these data, the results and any subsequent analysis of the data will be secured. They should also make clear who will have access and under what circumstances. *(May we share these results at national meetings this year? May we use the results of testing to develop your child's IEP next year?)*
- Any risks associated with data logging procedures should be explained in writing.

Research promise and current clinical practice

While the technical ability to record automated data logs is pretty much in place, clinically proven procedures for recording and analyzing the data have not yet been validated. And while this may not cause a problem with certain kinds of information, such as how many times a certain key was activated, other measures, including communication rate and types of language structures used, may require considerable testing and clinical trials to assure their validity.

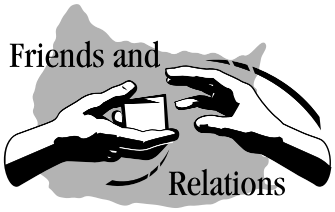
AAC professionals also need to consider carefully how to use this information in the best interest of the augmented speaker. Objective data may be prized by funding agencies, but unless it accurately reflects an individual's overall communication capabilities, premature dissemination of information about device output will not serve either the individual augmentative communicator or the augmentative communication community.

augmented communicators in their work is controlling their employees. The manufacturer of an augmentative communication device who considers the privacy of the augmented communicator in the design of the device is handing control to the device user. Very few people like to give up control; it makes their lives harder. Many people don't like to take control; it is too much responsibility. Ensuring privacy for augmentative communicators is a lot of work for everyone.

Privacy is a social, psychological, financial, legal and physical issue. Changing expectations, new technologies and expanding opportunities demand that augmented communicators, their families and the professionals who support them think about privacy boundaries and how to ensure they are respected for each individual.

CONFIDENTIALITY ISSUES IN SPEECH TO SPEECH

by Eda Wilson, SLP, Fort Atkinson Public Schools
and Bob Segalman, Ph.D.



Speech to Speech (STS) is now part of the Telecommunications Relay Service in 16 U.S. states and is also available in Sweden and Australia. As of March 1, 2001, the U.S. Federal Communications Commission (FCC) will require STS to be provided nationwide in the U.S.

How it works

To make a Speech to Speech telephone call, you first call a toll free STS number. You tell the Communication Assistant (CA) the number to call and the name of the person you wish to call. The CA identifies him/herself by identification number and places the call. Throughout the call, the CA repeats, or "revoices," exactly what the person with a speech disability says. Both parties say "GA," "go ahead," to indicate the other party's turn to talk.

The CA's job

According to Katherine Keller, in the Attainment Company video, *Speech to Speech*, "The CA doesn't interpret; the CA simply revoices verbatim what the person with the speech disability says. Everything that they hear in a phone call is held in absolute confidentiality; they can never repeat it."

STS policies

Communication Assistant training and practices help define confidentiality. Each telecommunication relay service has its own policies. The Wisconsin Relay System (WRS) brochure states: "All calls handled by the WRS are kept strictly confidential. As required by law, no relay employee can disclose information from a relay conversation, and no records of any relay conversation are saved in any format." CAs who breach confidentiality are fired.

FCC regulations

New FCC Regulations require Speech to Speech Communication Assistants in the U.S. to be able to save information for consumers by request between consecutive STS calls, but not between non-consecutive STS calls. Because talking can be very time and energy consuming for some STS consumers, the FCC is being asked to allow information to be saved between non-consecutive calls for 24 hours.

In the U.S., according to federal FCC regulations, "CAs are prohibited from disclosing the content of any relayed conversation regardless of content, and with a limited exception for STS CAs, from keeping records of the content of any conversation beyond the duration of a call, even if to do so would be inconsistent with state or local law. STS CAs may retain information from a particular call in order to facilitate the completion of consecutive calls, at the request of the user. The caller may request the STS CA to retain such information, or the CA may ask the caller if he wants the CA to repeat the same information during a subsequent call." The CA may assist the STS user as long as the user keeps control of the conversation and as long as the user does not object to such assistance.

A legal conflict

Trich Shipley, who works for the Minnesota Relay, wrote in message 214 of the Speech to Speech listserv that she discovered "a slight loophole in the ADA Law that requires that all relay calls to be 100% confidential." Trich explained the one exception to complete confidentiality. Only incidents that violate laws related to interstate or foreign communications may require CAs to divulge information and would allow a CA to be subpoenaed. Since no written documentation or records of calls are kept, there is nothing to be subpoenaed other than the CA. Under these circumstances, the CA would be required to state what he or she remembered of a particular call.

Conclusion

A person with a speech disability has more privacy during a Speech to Speech telephone call than a call made over a speakerphone or, of course, having another person make the call for them. Whether the call is a teenager asking a friend for a date or a taxpayer's call to the IRS, it is a basic right for people to keep their personal business personal.

A Word about Privacy

Privacy doesn't mean that you are the ONLY person to see, hear or know something. It means that you are the only person who has control over WHERE, WHEN, HOW and WHY you show or tell something to someone else. Here are some things you might want to keep private from someone, sometime:

Phone numbers
Addresses
Your SSN
Checking account numbers
Your dreams
Vocabulary in an AAC device
Keys
How to make your signature
Financial history and records
Medical history and records
Education history and records
Your age
Your marital status
Your disability
Your birthdate
Political affiliations
Photos of yourself
Photos of your things
Prayers
Details about your body
Whether you are home
Sexual experiences
Your fantasies
Falling in love
Email
Sexual partners
Pin numbers
Passwords
Your religion
Diaries
Journals
Correspondence
Spirituality
Personal dictionaries
Your opinions
Rental history at video store
Borrowing history at library
Who you were with
Videotape of you
Videotape of your stuff
Secret recipes
How you voted
Communication overlays
Reports about you
Receipts
Your phone calls
Your gender
Your money
What you bought
Who you date
How much you drink
Your conversations
Your life story
Your beliefs
Your sexual preferences
Your secrets
Where you've been

To protect your personal privacy

Before you share information about yourself or give anyone permission to collect data about you or share information about you,

Ask yourself

- Do I want them to have that information?
- Do they need that information?
- Will it benefit me if they have that information?
- Could giving that information to them harm me?

Ask them

- What is your purpose in requesting this information?
- How will your having this information benefit me?
- How will you use this information?
- With whom will you share this information?
- How and where will you store this information?
- How long will you keep this information?

Sources & Resources

Speech to Speech

Eda Wilson, SLP, Fort Atkinson Public Schools. edesw@yahoo.com

Bob Segalman, PhD., California STS, 1-800-854-7784 and ask for him at 1-916-263-8689. bob.segalman@att.net

The STS website, stsnews.com, lists all the STS access phone numbers and tells how to join the STS listserv.

Australia STS contact: Tom McCaul. Ace.Tom.McCaul@uq.net.au

Sweden STS contact: Inga.Svanfeld@tt.hoh.lul.se

The *Speech to Speech* video is published by the Attainment Company, P.O. box 930160, Verona, WI 53593-0160. 1-800-327-4269. To order the STS video, go to www.stsnews.com and click on "learn more about STS," or contact Brent Denu bdenu@attainment-inc.com at the Attainment Company.

AAC-RERC

http://www.aac-rerc.com
The AAC-RERC section is partially funded by the National Institute on Disability and Rehabilitation Research under grant number H133E9 0026. The opinions are those of the grantee and do not necessarily reflect those of the U.S. Department of Education. Published December 2000.

Privacy websites

Electronic Privacy Information Center
www.epic.org/privacy/internet/

Center for Democracy and Technology
www.cdt.org/privacy/

Platform for Privacy Preferences
www.w3.org/p3p

Automated data logging

Jeff Higginbotham, Ph.D.,122 Cary Hall, Department of Communicative Disorders and Sciences, University at Buffalo, Buffalo, New York 14214.
http://aac.buffalo.edu
cdsjeff@buffalo.edu

DynaVox system privacy

Rick Hohn, 1125 Cottontail Road, Vista, CA 92083. phone:760-598-8336
rickstalk@juno.com

DynaVox products are available from DynaVox Systems, Inc. 1-800-344-1778
www.sentient-sys.com

Thank you

To Brenda Klauditz for helping us to remember what is private.

Opt-Out?

It can be difficult for an augmented communicator to find safe, accessible storage for electronic data on a home computer, a telephone, a personal organizer or a communication device. It can be even more difficult to track who is collecting electronic information about you (as you surf the web, purchase by credit card, use your Blockbuster card, scan your purchases and swipe your health insurance card).

There are two ways of protecting consumers from unwanted electronic data collection. One is called "opt-out." This method leaves it up to the consumer to discover data is being collected and to let the data collectors know that the consumer is not willing to have his or her data collected. Most consumers do not opt-out; it's too hard.

The other method is called "opt-in." Opt-in emphasizes the individual's control over his or her electronic data. Opt-in demands that the data collectors ask each consumer's permission before collecting data or sharing it. American corporations are generally not fond of opt-in because opt-in hampers business; however, opt-in seems to be quite popular in Europe.

Consumer advocates recommend two more features which protect consumers from unwanted data collection: The consumer must be able to look at the collected data to see if it is correct, and the consumer must be able to change his or her mind about sharing information.

Protection of electronic data pits the ease of doing business against the rights of the individual consumer. Eventually there will be laws and regulations, but for now it's an electronic Wild, Wild West.

Opt-In!