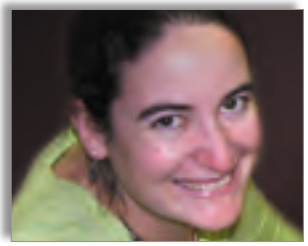
Connections

A Biannual Publication of
Washington Coalition of
Sexual Assault Programs

Volume XI, Number 4

SPRING | SUMMER 2009

TECHNOLOGY SAFETY



Toby Shulruff

Yahui Chi

EDITORIAL

Toby Shulruff, Resource Sharing Project
Yahui Chi, Tech Specialist

"The fast growth of phone and Internet technologies has made technology more and more a part of our everyday life. Technology changes how we think, how we work and how we relate to each other. Technology has been used in so many different ways in our movement. We see Sexual Assault Programs continually increase their online presence by establishing websites, and/or participating on MySpace, Facebook, YouTube and Twitter…etc. We see victims/survivors of sexual violence reaching out through technology to gain access to information. We see new victim services programs such as the Statewide Automated Victim Information and Notification (SAVIN) being used to provide notifications about offenders' release to crime victims via phone or email, and we see how GPS has been used to monitor sex offenders. It is important to understand that although technology offers new opportunities to provide resources and support to victims/survivors and to increase community safety, it can also be misused by abusers, give a false sense of security, and have dire consequences in the event of technology failure."

AS YAHUI WRITES IN HER ARTICLE IN this issue of Connections, technology has become increasingly intertwined with our daily lives and work. This issue focuses on some of the many implications of technology for survivors' safety and healing, as well as for our work as advocates. You'll find articles on stalking, evidence collection, assistive technology for people with disabilities, and technology in rural communities. We also examine a hot topic from the media – kids' safety online, and the rise of social networking sites. We've included some references and tools including statistics, resources for more information, talking points for advocates and teen safety tips.

As you read through this information and integrate it into your work, bear in mind that technology itself is just a tool. The dynamics of sexual assault, the behavior of offenders, and our own strategies to end sexual assault are still based on the same truths – what has changed is the speed and broader reach made possible through technologies. +

Connections

SPRING | SUMMER 2009
Volume XI, Number 4

Washington Coalition of
Sexual Assault Programs

THIS ISSUE:
TECHNOLOGY SAFETY

The Mission of the Washington Coalition of Sexual Assault Programs is to unite agencies engaged in the elimination of sexual violence through education, advocacy, victim services and social change.

Connections Magazine is published biannually and mailed to subscribing members of WCSAP. For membership information and to view articles online visit: **www.wcsap.org**

Design & Layout:
Debi Bodett
debi@debibodett.com

Table of Contents

STALKING, SEXUAL ASSAULT and Technology

By Caroline Palmer, JD

[***WCSAP: Stalking is a complex and often extremely dangerous crime that increasingly includes technology. Survivors of sexual assault who are also experiencing stalking need to be supported by advocates and other professionals with access to the latest information about technologies misused by stalkers. Caroline Palmer's article provides an important call to advocates to draw on our resources to support survivors of sexual assault and stalking.***]

TECHNOLOGY HAS BECOME SUCH AN integral part of our everyday lives that we often just take it for granted. Sophisticated multi-faceted cell phones allow us to make calls, send text messages and emails, check the internet, take photographs and schedule every minute of our lives. Laptop computers make it possible to work from anywhere through the web. We can contact friends and colleagues using social networking sites, remotely manage our finances through banking and credit card sites, manage complex projects with others across the country, or simply catch up on the news. Every time we leave our homes to make purchases, conduct business, or even engage in certain recreational activities we come into contact with technology that collects and stores our personal information.

Most of the time our interactions with technology are positive or at least fairly harmless. Although we should all worry about identity theft and excessive data collection, for the most part many of us engage electronically without fear, relying instead on the sort of informed skepticism that still allows us to accomplish what we want while using these helpful tools. On the other hand, victims and survivors of sexual assault who are also experiencing stalking are all too familiar with the seemingly infinite ways technology can be misused. In these cases informed skepticism must evolve, out of necessity, into extensive protective measures.

Every day we hear stories of sexual assaults and stalking accomplished through contacts made on Facebook or MySpace, the use of GPS technology to track someone's activities with the intent to harass, isolate and attack, the hijacking of personal computers to gather private information in order to facilitate stalking and harassment, the deployment of hidden video cameras to capture private activity, and the use of text messaging and other electronic communication to send upsetting and sometimes threatening messages. [*For more information see Kids' Online Safety article in this issue.*] According to the Bureau of Justice Statistics report, Stalking Victimization in the United States published in January 2009,

> More than one in four stalking victims reported some form of cyberstalking was used such as email (83%) or instant messaging (35%). Electronic monitoring was used to stalk one in 13 victims. Video or digital cameras were equally as likely as listening devices or bugs to be used to electronically monitor victims (46% and 42%). GPS technology comprised about a tenth of the electronic monitoring of stalking victims.

▶More than one in four stalking victims reported some form of cyberstalking was used such as email (83%) or instant messaging (35%). Electronic monitoring was used to stalk one in 13 victims. Video or digital cameras were equally as likely as listening devices or bugs to be used to electronically monitor victims (46% and 42%). GPS technology comprised about a tenth of the electronic monitoring of stalking victims.

It is clear that technology is playing a significant role in the commission of sexual assault and stalking crimes, and it is very likely the statistics will continue to rise as perpetrators become ever savvier about how technology can aid them in carrying out – and covering up – their criminal activities.

State and federal lawmakers struggle to keep up with changes in technology in order to provide an appropriate criminal justice system response when technology is used in cases of sexual assault and stalking. Computer crimes, harassment and stalking, interference with privacy, electronic surveillance, prohibitions on interception and disclosure of wire

or oral communications, and limitations on sex offender access to social networking sites are among the potential criminal penalties employed now in different states. Depending on the jurisdiction, there may also be civil liabilities available such as invasion of privacy. Government agencies are also aware of the growing problems – the Federal Trade Commission, for example, has become active lately in seeking restraining orders against companies who actively inform users how to employ their software for illegal or fraudulent purposes.

Despite the best efforts of all branches of government and their good-citizen partners in the corporate sector, the law evolves slowly as compared to the always-innovating for-profit technology sector and the people who use its advances for criminal purposes. Law enforcement and prosecutors are constantly working to find creative and current ways to respond to new infractions of the law presented by unanticipated uses of technology. For example, "sexting," the distribution of sexually explicit images by cell phone, has become particularly prevalent among young people. When the images are forwarded beyond the intended recipient – sometimes to cell phone users throughout entire schools – the results can be emotionally devastating. The person in the picture may never have intended more than one person (or perhaps anyone) to view it. Distributing the picture can sometimes, but not always, lead to serious charges for the sender, including dissemination of child pornography.

Using resources and advice, not to mention a willingness to stay abreast of major changes in technology use and misuse, advocates can help victims and survivors learn how to better equip themselves to deal with perpetrators who use technology to further their sexual assault and stalking crimes. Monitoring cell phone use and location, for example, can deter a stalker from downloading a GPS tracking program that will allow him to follow a victim from place to place. Avoiding unknown email attachments and denying access to personal computers by others can thwart opportunities for perpetrators to load spyware software or keystroke logging hardware. These spyware tools can make it possible for a stalker to monitor computer usage either remotely or on site, including the capability to take screen shots that will show email communication, web sites searched, and other private information. Use of complex passwords integrating numbers, letters and symbols can make it more difficult for others to guess at a more familiar term; changing passwords on a regular basis provides yet another layer of security. Taking pictures of harassing and threatening text messages and sharing them with law enforcement is particularly important. Cell phone carriers do not often archive messages for long and even if law enforcement tries to obtain information by court order, the sought-after messages may already be gone from the provider's system. Some companies are changing their policies with regard to keeping messages but for the most part the major carriers still do not hold them much longer than 24 hours. [*For more information, see Evidence Collection article in this issue.*]

Unfortunately these best efforts are not always enough and victims and survivors must resort to other, more extreme methods to protect themselves, including using a safer computer to engage in personal communication and research for services, using an alternative cell phone or other phones for calls to supportive or other resources, or, in some cases, seriously limiting their use of technology altogether. Such dire measures are not only inconvenient and stress-inducing, but can also, paradoxically, decrease safety in some cases, so it is important to plan accordingly for such contingencies.

Technology offers many positives to victims and survivors of stalking and sexual assault. It can be a helpful tool for providing services, and often victims and survivors network online, providing personal support to one another and working together toward system change to prevent sexual violence. The world is an increasingly wired place and there is much to be gained from the connectivity cell phones, computers, and other smart tools offer to all of us. It is easy to feel overwhelmed by all of the potential for good that exists from technology – and all of the potential for bad. Still, by working together, advocates, law enforcement, prosecutors and the good geeks among us can stay informed, work to keep the laws up to date, and continually share this information with the victims and survivors of stalking and sexual assault who need it most. +

Caroline Palmer is the staff attorney at the Minnesota Coalition Against Sexual Assault where she works on public policy issues, provides technical assistance, and develops trainings and materials for advocates and attorneys. She is a graduate of Hamline University School of Law and Barnard College.

EVIDENCE COLLECTION
In Stalking Cases

By Detective Rande Christiansen

[WCSAP: Related to the previous article, Det. Christiansen shares a law enforcement perspective on the collection and preservation of evidence in stalking cases that include technology. Some of these guidelines will also apply to similar cases of harassment. As he points out in this article, stalking cases are so varied and complex, that it is crucial for advocates to share with survivors information about evidence collection for a possible criminal case, and to support them in making crucial decisions about their safety.]

"EVIDENCE COLLECTION" IS A TERM usually reserved for law enforcement and most training on this topic is devoted to them. We need to understand that cases that involve obtaining and collecting technological evidence also involve the victim and advocates. Many times victims being stalked are not terrorized by just the old fashioned ways of following and surveillance, but now also with technology. This can vary from emails, text messages, instant messages, and using various Internet sites (i.e. MySpace, Facebook, etc.) to monitor the victim. We need to advise victims correctly for both evidence collection and safety, with technology being so prevalent.

Cell phones in urban and now in rural areas are common. Many households now use the cell phone as the primary line opposed to a hard-wired line. Victims carry their phones "everywhere" they go, and can now be monitored by various means. Cell phones can be monitored or tracked with GPS, Bluetooth, or other functions now available on the phones. If a victim believes this is happening, they should consider turning off certain functions on the phone. If possible and economical, victims should discontinue use of that phone and get a new service through another carrier with security access only by the victim.

While doing instruction of investigation of stalking cases, one of my main points is not to have the victim change their phone number. In years past, the advice was to have victims change their number and the stalker would just move on. The advice that I now give incorporates both evidence collection and safety. Changing their number can be problematic in that the number probably will be released or found on the Internet. The "evidence" in the form of text and voice messages will be lost in most cases if the victim changes the phone number. The major safety reason for not changing the number is that once the number becomes "unpublished" or not available to the stalker, there is a high probability that the stalker will try to find the victim in person to give his/her message.

Text messages have an extremely short retention period with the service providers, so that even law enforcement may not be able to collect them for evidence in time. Victims should be instructed that the messages need to be downloaded by a forensic expert, or in most cases digitally photographed for preservation. Law enforcement should take these photos for proper chain of evidence, and so as not to put advocates in the position of a being called as a witness for the case. Most phones now seem to have large storage capability, but when maximum capacity is reached the older messages, both text and

voice, will be eliminated. Another point of retaining and recording text and voice messages will assist persons tasked with threat assessment to read and interpret possible future problems and actions of the stalker.

Previous research studies of stalking behavior used to show that following and surveillance were at the top of the list and the use of technology was low. I have found that working stalking cases now, most, if not all, involve the use of some type of technology harassment. Many of the cases that are presented to the street Officer did not mention any emails or similar harassment as part of the case. I have found that many victims need to be asked if they have received the unwanted technology contact as part of the harassment/stalking. Many don't mention this in the original report unless asked.

The primary report may list the stalking behavior to the effect, "He hacked into my MySpace account," as many of the victims are college age or young adults. It is a necessity nowadays to be familiar with the various Internet sites to include MySpace, Facebook, etc., when giving advice on either preservation of evidence or collection for prosecution.

One very good thing about technology is the response suspects give to victims telling them to "leave me alone." In almost all cases I have investigated, when the victim sends an email, text message, instant message or other electronic message to "leave me alone," the stalker will usually respond. Saving and preserving this response is imperative for victims to show that the suspect was told the contact is unwanted, but also starts a time line in investigations for stalking if it continues. This also involves a protective factor, in that the victim doesn't have to see the stalker in person to deliver the message.

Service providers and technology experts advise victims to delete any unknown or unsolicited email. This is extremely valuable advice except in stalking cases. Listen to the victims in these cases, and when they receive a "strange," unsolicited, or masked email they believe is from the stalker, they are probably right. Then comes the double-edged sword advice of "to open or not to open." Opening one of the emails may give rise to the possibility of infecting their computer with viruses or other infections.

Opening one of these emails may also be the route by which a stalker infects the victim's computer with a type of spyware without their knowledge. The information presented here is not a secret and has widespread usage to track victims. The problem is that if victims use a type of spyware detection software, it will generally find, quarantine, and wipe out any of the "evidence" needed for proof of where the information is being sent. The actual analysis should be completed by a computer expert that can collect, document, and testify on the information located, if a victim believes that their computer is infected with spyware. The problem is in finding someone to do the analysis, since most law enforcement departments may have limited or no services to complete the analysis. The criteria for accepting a computer for this analysis will require more than, "he hacked into my MySpace account."

◀It is a necessity nowadays to be familiar with the various Internet sites to include MySpace, Facebook, etc., when giving advice on either preservation of evidence or collection for prosecution.

As a law enforcement investigator I think the one thing that I would work to take away is the "DELETE" button. In hundreds of cases I have heard the victim state to the effect, "I just couldn't listen to his voice anymore," or "I just couldn't take one more text", so she deleted the "evidence." We need to understand that victims hitting the "DELETE" button is a coping mechanism, and assist in educating victims that not using the button may increase their survival or get the stalking to stop.

Technology is here to stay, and it is imperative that as either advocates or law enforcement giving victim safety information, we must have basic understandings of the function and preservation of evidence. Armed with the basic information and resources, this will empower victims to gain back their sense of normalcy in these cases where technology has invaded their lives. +

Detective Christiansen has been with the Seattle Police Department for 19 years. He has been a Detective in the Domestic Violence Unit for 13 years, with majority of cases involving harassment and stalking.

THE HISTORY OF TECHNOLOGY

and How it Relates to the Movement Against Sexual Violence

By North Carolina Coalition Against Sexual Assault

▶In her book The Chalice and the Blade, Riane Eisler, speaks of a time when men and women were equals, a time when there was no violence, a time when people respected each other and treated each other with kindness and dignity.

Something happened between Minoan times and today. Violence is commonplace. As technology advances we are not only given the opportunity to increase our safety and provide better services for survivors of sexual violence, but to change the very society that we live in.

In the early 1800s Harriet Ann Jacobs told her owner who was threatening her and demanding sexual favors, "You have tried to kill me, and I wish you had; but you have no right to do as you like with me." Harriet's technology was her voice and she used it! She took a stand and said, "This is not right"!

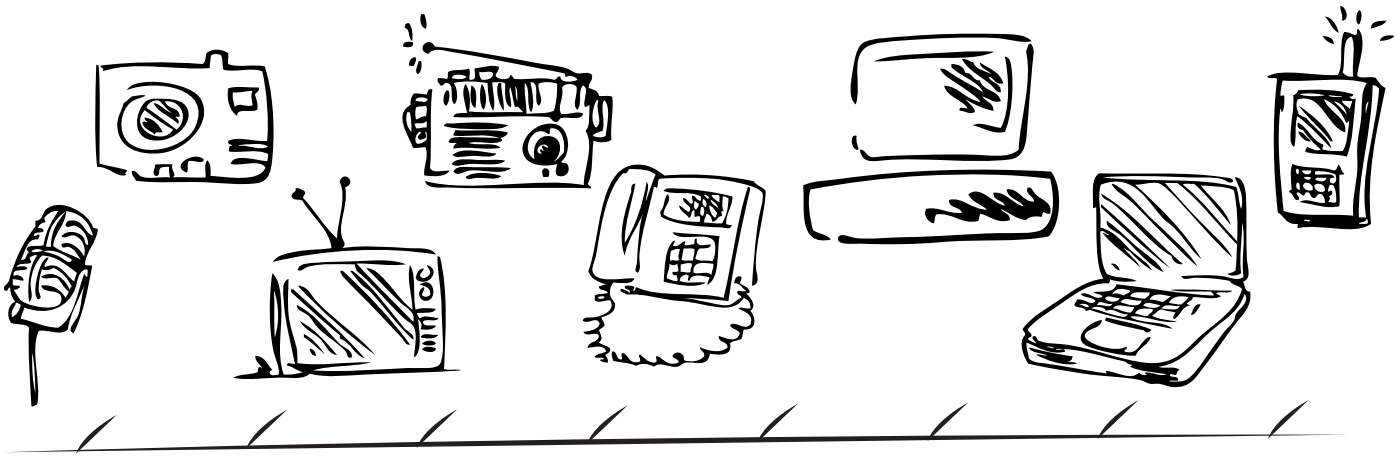
WHILE TECHNOLOGY AND THE USE OF technology in the Rape Crisis Movement has not evolved at the same pace over the years, there are many inventions that have become imperative for the movement.

In 1827, it took Joseph Nicephore Niepce 8 hours to take the first photograph. By 1947 Polaroid came out with its first instant camera and in 1963 color film emerged, leading to the Polaroid Macro 5 SLR and 15 Spectra AF cameras now used to document injuries in sexual assault patients. The colposcope was developed in 1925 and the computer aided colposcope in 1988 allowing forensic nurses to detect minute genital trauma in the cervix, vagina and vulva. More recent advances in digital imaging and camera technology have made it possible to reduce the cost and discomfort of pictures used for evidence in sexual assault forensic exams.

In 1876 Alexander Graham Bell and Elisha Gray raced to patent the first telephone allowing Rape Crisis Centers to provide 24 hour, 7 day a week hotlines for survivors of sexual violence and to communicate with one another to provide improved services to the individuals they serve.

In 1973 Chester Carlson invented the Xerography now used throughout the Rape Movement to mass produce information to educate members, allied professionals, and make duplicate records of client information when subpoenaed to submit information to the courts.

The FCC approved cell phones in 1982 (pagers were approved in 1958), ultimately allowing Rape Crisis Centers to provide 24-hour hotlines without having someone physically at a phone. Doctors and nurses could now be on call to provide rapid medical attention to patients. The cell phone also has allowed individuals to feel a sense of safety. Though cell phone



coverage areas are improving, it remains important for victims to give their location immediately when calling 911.

The mid-80's brought about many new advances in DNA technologies, two of the big ones being Restriction Fragment Length Polymorphism (RFLP) and Polymerase Chain Reaction (PCR). PCR in particular allowed for DNA amplification of very small amounts of sample. This technology would later walk hand in hand with UKDNA database (1995) and the United States' Combined DNA Index System (CODIS, 1998). DNA results could now be entered into a DNA database and the sample could be compared with known criminals in the database. These technologies led to the reopening of several sexual assault cases that could not be prosecuted before. In January of 2000, the NY City Police Commissioner reopened 12,000 unsolved rape cases. These technologies have also led to the release of falsely convicted prisoners.

Rap Tomlinson created the first e-mail program in 1972, allowing for information to be sent quickly over long distances. Today, this allows us to share documents, correspondence, and spread information at rates that were until this point unimaginable. Many times e-mail is quicker than picking up the telephone and it does not incur any long distance charges like the telephone or fax. Because e-mail can be sent or reviewed at one's leisure, it also allows us to communicate with professionals in other time zones without worrying about the time of day.

In 1991 CERN released the "World Wide Web," the first Graphic User Interface (GUI) software developed by Tim Berners-Lee. The introduction of the "www" with user friendly browsers and email has opened a new door for the Rape Crisis Movement. Many rape crisis centers and most coalitions now have websites and email accounts. +

◀Looking back on what individuals and groups have accomplished with the technology available to them at the time, can you imagine what we can accomplish if we put into use all the technologies we have today!

It is important that as we move forward we do not forget the technologies we've used so successfully in the past either on their own or incorporated with our newer technologies. I encourage everyone to remember to use your voice and speak out against sexual violence.

5 WAYS
TO MAKE SEXUAL ASSAULT SERVICES
More Accessible Using Assistive Technology

By Cynthia Fraser

[WCSAP: People with disabilities and people who are Deaf or hard-of-hearing experience an extremely high rate of sexual assault, and often encounter additional barriers to safety and healing. As we work to support survivors through advocacy and partnerships, it is important that we increase our knowledge of the technology used by people with disabilities or who are Deaf.]

ASSISTIVE TECHNOLOGY HAS TRANSFORMED THE lives of many people with disabilities. Assistive devices and services are often essential to creating an accessible work or school environment. Assistive technology has quickly become a critical component in ensuring that sexual assault programs provide accessible services for victims of sexual violence. Here are five ways sexual assault programs can increase safety and accessibility for survivors by using assistive technology:

STEP 1

Educate yourself: Learn how assistive technologies benefit individuals who are Deaf or have disabilities.

There are many types of assistive technology. It can be any device, equipment, product, item, or service that maintains or increases access; decreases or removes systemic barriers; or, supports accessibility, autonomy, and self-determination for individuals with disabilities or who are Deaf.

Some people with physical or motor disabilities might want to use mobility devices, such as wheelchairs, or computer software and equipment to facilitate communication and daily living. Voice synthesizers enable someone's computer to speak what they typed; speech recognition, point-of-gaze software, and orally controlled mouthsticks support hands-free computer access. Tiny tilt-sensitive sensors worn on the body can be used to control a computer or living environment (to turn on/off air conditioning or lights).

Some individuals with cognitive disabilities might want to use communication aids that associate simple images with phrases; these can be customized with images that help a sexual assault survivor more comfortably point out the violence

they experienced. Sexual violence survivors who have memory loss due to head or brain injuries, depression, chronic pain, amnesia, sexual abuse, or other reasons, may like to use inexpensive portable memory joggers to record audio messages when certain things happen, or to remind themselves of routine tasks.

People who are Deaf or have hearing and/or speech disabilities might reach out for support using free, confidential Telecommunication Relay Services such as: Text-to-Voice T-T-Y Relay, Voice Carry Over, Hearing Carry Over, Speech-to-Speech, Shared Non-English Language, Captioned Telephone, and Video- and IP- Relay Services. Some people who are Deaf or hard-of-hearing may prefer to communicate in sign language over a high-speed cable or internet-connected Video Phone, video relay service or video remote interpreter. Others may prefer to contact your agency by typing on a T-T-Y (teletypewriter or text telephone) device connecting through their phone line. If your agency has a dedicated T-T-Y line, they can directly call your agency's T-T-Y number; if not they can reach you via a relay service. Learn more at Washington Relay Services: www.washingtonrelay.com

People who are Deaf-Blind might use Braille T-T-Y devices to reach you, with or without a relay operator. Hand-held devices that serve up emails via a refreshable Braille keyboard that moves under someone's fingertips, and screen readers that speak text aloud or convert text to Braille can increase accessibility for people who are blind or have low vision. GPS Location Orientation devices that plot routes and download maps in speech or Braille enable someone who is blind to get directions read aloud as they move. Learn more at American Foundation for the Blind AT Product database: http://www.afb.org/prodMain.asp

Any popular technology can be considered assistive if it increases safety and accessibility for people who: are Deaf or hard-of-hearing; are blind or have low vision; have cognitive/developmental or physical/motor disabilities; have mental or psychiatric disabilities, or multiple or invisible disabilities. Sexual assault program staff should receive regular training on popular and emerging assistive technologies so they competently understand assistive devices a survivor may use or need to acquire.

STEP 2

Discuss privacy and safety risks with survivors, including how sexual violence perpetrators can misuse assistive technologies.

If a sexual violence perpetrator has physical or remote access to an assistive device or service a survivor uses, it may be risky for the survivor to use that device to seek help. Many perpetrators monitor or intercept the victim's communications to groom, coerce or stalk. Some perpetrators break and tamper with assistive devices, or purposely hurt the victim so they can't use their assistive technoloy device (e.g. break a victim's fingers or hand). Perpetrators misuse communication devices, such as a T-T-Y machine or Relay services, to impersonate the victim. Abusers may tamper with internet accessibility tools and devices (such as screen readers) to limit or prevent a victim's ability to search online for resources, contact services, or communicate with others. For example, they may change computer settings to shut off sound, decrease magnification, or remove other accessibility programs.

Sexual assault programs should find safe ways to strategize with survivors about how perpetrators misuse assistive technology. For example, to decrease impersonation via Relay or T-T-Y, agencies can ask the victim to create and use a code phrase that only the victim and the advocate know. Your agency may need to help a survivor get replacement devices, and/or get law enforcement to document how the devices were tampered with or destroyed. Sexual assault program staff should receive ongoing training about risks and take steps to increase the safer use of technology in their daily work.

STEP 3

Conduct accessibility assessments of your sexual assault program. Identify barriers that keep victims from fully accessing services. Commit to immediate steps, longer term activities, and a strategic plan with the goal of eliminating barriers.

The Americans with Disabilities Act (ADA) mandates that sexual assault programs be accessible to people with disabilities; assistive technology is necessary to achieve this. Agencies are strongly encouraged to do a comprehensive accessibility audit and identify assistive technology that can decrease barriers. For example, door bells and fire alarms can be set to vibrate or flash lights for people who are Deaf, or to make sounds and disable lights for people with epilepsy. Agencies can install and advertise a dedicated T-T-Y line, and provide both in-person and remote video interpreter service options for survivors who are Deaf or hard-of-hearing.

If your sexual assault agency has a website, posts

information online, or, offers in person computer services, it is important to provide software or assistive devices that ensure accessibility to all clients. To ensure all assistive devices can fully access your website, your website may need to be altered so users can easily increase font size, magnify a webpage, change colors, hear text descriptions of image files, and more. You can begin testing your website accessibility using a variety of free online web accessibility checkers (e.g. http://wave.webaim.org) or screen readers (e.g. http://webanywhere.cs.washington.edu). Be sure to budget for ways to maintain and further increase website accessibility, do follow-up evaluations, and then, ask people with various disabilities to test your progress.

Technology will continue to evolve; agencies should regularly ask, identify and add assistive technology that increases options for individual survivors with disabilities.

STEP 4

Support the rights of each sexual violence survivor to access the assistive technology that best meets their needs and preferences.

Publicize the ways you have become accessible and state that your program will provide accommodations upon request. Be sure to budget for those requests, but never make assumptions about what an individual will prefer or need. For example, one victim who is blind may want you to make mp3 audio files of your brochures for her iPod, another may want to hear them using a screen reader on a computer, and another may want to read them in paper or electronic Braille.

When sexual assault survivors first contact you, they may not have the assistive technology they prefer or need. Support their right to test multiple devices, to decide which devices best meet their needs, and to access funding options to purchase the necessary devices. Many assistive technology tools and web designers cost more money than your agency or survivors can afford. This is why it is critical to partner with agencies that help people access affordable assistive technology.

STEP 5

Collaborate with disability rights organizations, Independent Living Centers, Assistive Technology agencies, and other groups to ensure you can meet the needs of people who are Deaf or have disabilities.

These organizations are critical partners in your work to ensure that survivors get access to the assistive technology they need. They should be able to help you understand and access the available public and private loans, grants and subsidies that may defray costs for one or more devices someone needs. You should work to establish and formalize relationships with these agencies, for example through cross-training of staff and volunteers.

- **Washington Assistive Technology Act Program** (http://watap.org/) serves all Washington residents seeking information about assistive technology and accessible information technology. For funding help, see http://watap.org/funding/index.htm
- **Washington Access Fund** (http://www.watf.org) promotes access to technology and economic opportunity for individuals with disabilities. They provide rentals, loans and matched savings accounts (to low income households) for assistive technology.
- **Abused Deaf Women's Advocacy Services** (http://www.adwas.org) provides services to Deaf and Deaf-Blind victims of sexual assault and/or domestic violence.
- **Deaf Access Washington** (http://www.dawash.org/) works to ensure that Deaf and Deafblind consumers have equal and appropriate access to their communities, vocational opportunities, counseling services, education and to public and private services.
- **Washington State Independent Living Council** (http://wasilc.org/) promotes independent living for persons with disabilities. Centers for Independent Living (CILs) are grassroots, advocacy-driven organizations run by and for people with disabilities. All Centers provide individual and systems advocacy, information and referrals, peer support, and independent living skills training.

With thanks to Erica Olsen.

Cynthia Fraser is a Technology Safety Specialist with Safety Net: The National Safe & Strategic Technology Project at the National Network to End Domestic Violence. Through training, technical assistance, and policy advocacy, she addresses how technology impacts survivors of stalking, domestic and sexual violence. She has 18 years experience working to end violence in the US and Canada at local hotline, shelter, court, and victim advocacy organizations as well as nationally at organizations such as the US Institute for Women's Policy Research.

Rural Challenges
IN A DIGITAL WORLD

By Teresa Atkinson

[WCSAP: Access to technology looks different in urban and rural communities. As a result, our work as advocates and survivors' day-to-day experience of technology also vary depending on the size and geographic isolation of a community. In this article, Teresa Atkinson discusses technology in rural areas and what that means for our work.]

RURAL AREAS HAVE AN AMAZING AND fascinating infrastructure that in many ways mirrors the technology we have available today. I grew up in a small, rural town in Northern Idaho (population 395) in the early'70s and'80s, where we had blogs, high-speed communication devices, spyware, spycams, and social networking long before computers and the Internet. The devices were not stand-alone, they were integrated and connected. They were known as the local newspaper, town gossips, and the local café.

Every Wednesday, the local paper would catch you up on what friends and relatives were doing by reading the "On the Ridge" section. Much like a blog, it would detail the happenings of people's lives. Often it would list the names of those who attended events at someone's house, who went on vacation, who had out-of-town guests and what they did to entertain them. Also, many of the farmers just outside of town were still on "party lines" (a single phone line connected to two or three pouses). Each house had a

separate ring sequence to indicate which house was being contacted. Hacking into the system required no installation of spyware or breaking of password codes. Wire tapping at its best – just pick up your phone quietly and listen in on your neighbors' calls. News traveled fast once it reached the high-speed lips of those in town who continued to spread the news.

The local café was the hub for social networking and intelligence gathering. My father would walk down to the café every Saturday morning for coffee, then come home and tell each of us kids what we had done on Friday night – with detailed accuracy. We didn't have a town cop; the citizens were the enforcers in times of need. To this day, like in many small towns, that infrastructure remains. Technology, however, continues to change and challenge an older way of life.

▶ One barrier stands out above the others – the perceived value of having and accessing high-speed Internet connection was not always readily seen by the community.

As advocates reach out and work with rural survivors, small town assumptions need to be evaluated. Times change and so does our way of communicating. The town "grapevine" may still be in place, but that doesn't mean word of mouth is the only source of information. Most schools in small areas have broad band internet connection. Many areas now have cellular towers for cell phone service, and many farmers and hand crafters are selling their goods through their websites as well as their local farmer's market. If we assume they are under resourced in their ability to utilize technology, we may miss the opportunity to provide outreach and services.

A 2008 Pew Internet and American Life Project report found that 55% of American adults nationwide have access to broadband or high-speed Internet. In rural areas, about 38% have broadband in their home. In Washington State, by comparison, approximately 72% of residents in 5 rural counties (Columbia, Ferry, Grays Harbor, Lewis, Stevens) have Internet access, yet only 32% of those residents have broadband service, according to a 2008 Washington Utilities and Trade Commission (WUTC) study. Dial-up is not dead quite yet.

The WUTC study found technology barriers that rural communities face include lack of service availability, high cost of service, and lack of viable and multiple competing options. Yet one barrier stands out above the others –the perceived value of having and accessing high-speed Internet connection was not always readily seen by the community. So, just because you build it, doesn't mean they will come. Rural communities are not necessarily resistant to change, but they do need an opportunity to see and understand how technology and access can improve their lives, their businesses, and their community as a whole.

In these days of economic uncertainty, getting connected to the Internet could realistically build a more educated and skilled workforce through online training or webinars. There is also potential to create new businesses or new markets for products, goods or services through access to a larger audience online. Internet access can be used to increase academic performance and literacy in school, and connect people with resources, information and services. It can transform health care through the ability to email digital test reports and images to larger hospitals or research facilities for further diagnosis. It can provide a tool for participation in community organizing and

meaningful. Rural areas tend to be (but not always) more disconnected from resources and services due to their isolated location, yet encompass many diverse population needs that may not be adequately addressed locally. Engaging schools and libraries, as well as investing in new community technology centers, will/could provide opportunities for citizens to have adequate online access and updated hardware and software. Developing resources in these community settings and offering individual or group instruction can create a positive experience in a learning environment.

Social service agencies and nonprofits can supplement efforts toward digital inclusion by working with their local communities to address additional barriers to client participation such as child care, negotiating extended and flexible hours for technology centers or access points, and assisting with transportation issues for participants.

▲Developing resources in these community settings and offering individual or group instruction can create a positive experience in a learning environment.

activism as well as the ability to connect to others for support – down the street or across the globe.

In Washington State, Communities Connect Network has been instrumental in helping frame community technology and access for underserved populations. CCN is a statewide coalition of public and private organizations working to ensure that Washington State is a leader in "digital inclusion".

Digital inclusion encompasses three key components: 1) providing access to computers and the Internet at reasonable costs and ease of connectivity; 2) literacy or skill building in using computers and Internet technologies; and 3) useful content and services that are culturally and educationally appropriate and target lower-capacity residents and underserved populations. The backbone of implementing a plan involves the deployment of broadband to rural areas and creating equity in access and use. The strategy is to involve the community and build on any existing programs to help reach a higher level of online connectivity for residents.

The expense of computer equipment and upkeep required to safely access the Internet and utilize other software programs for skill-building puts low-income and rural areas at a disadvantage. Many residents lack the skill or literacy to make an Internet connection

As broadband initiatives sweep the nation as part of the Obama Administration's efforts to create jobs and combat the digital divide, it is time to be informed and take action. Ready or not, changes are coming. To take advantage of the benefits technology can bring, more than just broadband Internet access needs to be provided. Digital inclusion is by no means an equalizer for underserved populations. It does, however, provide opportunities to lessen the gap. Individuals, families and communities will benefit, if the value is demonstrated and the support structure for success is in place. +

Teresa Atkinson is the Technology Safety Project Program Coordinator for the Washington State Coalition Against Domestic Violence. She currently manages a federal grant from the Office on Violence Against Women in cooperation with NNEDV's Safety Net Project that provides training and technical assistance to nine western states DV and SA coalitions and their members on technology safety and technology-related stalking.

USING TECHNOLOGY

as an Advocacy Tool and Understanding Implications for Victim/Survivor Safety

By Yahui Chi

[*WCSAP: As advocates, we work directly with survivors and communities. We also work to promote social change. Many new technologies challenge our traditional understanding of social change work, while also increasing the opportunities for rapidly and inexpensively spreading our message.*]

THE FAST GROWTH OF PHONE AND INTERNET technologies has made technology more and more a part of our everyday life. Technology changes how we think, how we work and how we relate to each other. Technology has been used in so many different ways in our movement. We see Sexual Assault Programs continually increase their online presence by establishing websites, and/or participating on MySpace, Facebook, YouTube and Twitter…etc. We see victims/survivors of sexual violence reaching out through technology to gain access to information. We see new victim services programs such as the Statewide Automated Victim Information and Notification (SAVIN) being used to provide notifications about offenders' release to crime victims via phone or email, and we see how GPS has been used to monitor sex offenders. It is important to understand that although technology offers new opportunities to provide resources and support to victims/survivors and to increase community safety, it can also be misused by abusers, give a false sense of security, and have dire consequences in the event of technology failure.

According to Internet World Stats, Internet usage in America has grown from 44% of the population in 2000 to 73% of the population in 2008. The increase in Internet usage along with how people change the way they use the World Wide Web has influenced the shift to Web 2.0. "Web 1.0" was about proprietary information, a Webmaster was the primary person for updating the read-only content, and most Web pages were static. Web 2.0 uses the Web to facilitate communication. It encourages users to actively create their own content in the form of text, videos, audios or graphics. It creates online communities and prompts social networking. It is user-friendly, very customizable and require minimal technical skills. As social change organizations, in order to use the Internet as an effective tool to prevent and to end sexual violence, we need to be aware of what the current Web culture is and be willing to adopt emerging technology in order to develop the best strategies to end sexual violence. Successful online organizing and mobilizing is powerful. It empowers each individual to take the lead as an organizer for a common goal and reduces the traditional outreach method cost. For example, Stop Family Violence, by using the Internet, within 3 months was able to organize people from across the nation to send more than 164,000 messages and made numerous phone calls to Congress during VAWA's reauthorization. Facebook users formed a pro-privacy group that organizes against applications that automatically share users' information on Facebook. The group has grown to over 80,000 members and as a result, Facebook reversed its policy. As we continue to witness how technology has been used as a tool to make a difference, our movement's vision needs to expand to include using technology as one of the mediums to end sexual violence.

In the United States, 1 in 6 women reported experiencing an attempted or completed rape at some time in their lives, according to the National Violence Against Women Survey. According to a December 2008 survey by the Pew Internet & America Life Project, 75% of adult women use the Internet and almost half of all Internet users now use

search engines on a typical day. There are significant numbers of victims/survivors seeking information, resources, and support online. If your organization has an online presence, victims/survivors might contact you without knowing the potential risks. There are many steps an organization can build into its website to protect victims/survivors' safety. We can post brief technology safety tips on every page of the website to remind victims/survivors that the online activities are being stored on their computer; and we can use web forms to allow visitors to contact us instead of posting staff's email addresses. Organizations should also have policies and procedures addressing how to respond to victims/survivors' emails. Whenever possible, Community Sexual Assault Programs should work to acquire their own mail server instead of using the free web mail applications such as Hotmail, Gmail or Yahoo Mail in order to better protect the electronic communications received from victims/survivors. Additionally, organizations also need to be mindful about what content is appropriate to post on a website. Some tools are best used in-person, and are just not as effective on the web.

While our movement continues to offer resources online, it is crucial to make sure the services are accessible and available to everyone. The December 2008 Pew Internet & American Life Project indicates that:

- 77% of Whites and Non-Hispanics have Internet access versus 58% of Hispanics,
- 71% of people who live in urban areas have Internet access versus 63% in rural areas,
- 94% of households with income greater than $75,000 have Internet access versus 57% of households with less than $30,000, and
- 95% of people who have a college degree have Internet access versus 35% of people who have less than a High School diploma.

To better serve all communities, we need to be aware of the Digital Divide - a term that refers to the gap between people with effective access to digital and information technology and those with very limited or no access at all (Wikipedia). The Internet has broken down the traditional geographic barriers and provides rural communities a way to be connected with the rest of the world. Technologies including the Internet also provide greater access to information and resources for people with physical disabilities. However, we still have community members that are not benefiting from this innovative technology. As we move forward in the digital era, we need to make sure our information and services reach both online and offline community members. For example, as we invite them to join our mailing list, provide options for either email or snail mail.

◀To better serve all communities, we need to be aware of the Digital Divide - a term that refers to the gap between people with effective access to digital and information technology and those with very limited or no access at all (Wikipedia).

As we strive to provide professional quality service to victims/survivors, we need to constantly evaluate technology safety at the organizational level. When we remind victims/survivors to change their passwords often, we too need to change our own passwords often. We will make sure the victims/survivors' data is locked in a room that only authorized persons can access, we will purge electronic records according to our retention and destruction policy, and we will make sure any consultants who have access to victims/survivors data sign confidentiality agreements. Moreover, we should practice collecting a minimum of victims/survivors' personal information, removing any identifying information when we need to forward an email to staff, and we should not save confidential information on personal computers or storage devices like USB drives. It is very exciting to see how much technology has benefited our work. However, before we adopt new ways of communication and service delivery, we must first evaluate how it will impact victims/survivors' privacy, confidentiality, and safety. +

Yahui is the Technology Specialist for the Washington Coalition of Sexual Assault Programs. She is responsible for the operation and management of the agency's technology infrastructure and she is currently working on the Washington Violence Against Women Network project. She provides technical assistance and trainings on technology safety.

KIDS' SAFETY ONLINE:

From the Crimes Against Children Research Center

By Toby Shulruff

▶Our common-sense notions of online risk and online predators are inaccurate.

FEARS ABOUT "ONLINE PREDATORS" HAVE grown quickly as the Internet has spread through American households, libraries and schools. Understanding the reality and dynamics of risks and violence that kids face online is crucial in our work to support survivors and prevent sexual violence. Policy and practice are largely guided by inaccurate portrayals of the scope and nature of the problem. As a result, increasingly scarce resources are misdirected, and more importantly, families and children do not have accurate information with which to make decisions.

Eminent child sexual abuse researcher David Finklehor and his colleagues at the Crimes Against Children Research Center have clearly stated that our common-sense notions of online risk and online predators are inaccurate.

➲DON'T SAY:

1 in 7 youth is contacted by an Internet predator.

This most commonly used statistic from the widely cited Youth Internet Safety Survey (YISS) counts, "unwanted sexual solicitations," but many such experiences are probably not encounters with true Internet sex offenders. For example, many of the youngsters thought the solicitations were from other youth or just casual rude comments.[1]

➲DO SAY:

1 in 25 youth in one year received an online sexual solicitation where the solicitor tried to make offline contact.

Four percent of the youth in the YISS received solicitations in which the solicitor made or tried to make contact with the youth offline via telephone, offline mail or in person.[1] These are the online encounters most likely to lead to an offline sex crime.

➲DON'T SAY:

Internet predators pretend to be other youth to lure victims into meetings.

In the vast majority of Internet sex crimes against young people, offenders did not actually deceive youth about the fact that they were adults who had sexual intentions. Acknowledging that they were older, the offenders seduced youth by being understanding, sympathetic, flattering, and by appealing to young people's interest in romance, sex and adventure.[2]

➲DO SAY:

Internet offenders manipulate young people into criminal sexual relationships by appealing to young people's desire to be appreciated, understood, take risks, and find out about sex.

To warn youth and parents about these crimes, we need to educate them about the real dynamics, and how naïve romantic illusions make some young people vulnerable to adult offenders who use flattery and seduction.

[1]Wolak J, Mitchell K, Finkelhor D. Online victimization: 5 years later. Alexandria, VA: National Center for Missing & Exploited Children; 2006. Available at: http://www.unh.edu/ccrc/pdf/CV138.pdf.

[2]Wolak J, Finkelhor D, Mitchell KJ. Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. Journal of Adolescent Health 2004;35(5):424.e11-424.e20.

➲DON'T SAY:

Internet predators lure children to meetings where they abduct, rape or even murder.

Although cases of abduction, forcible rape and murder have occurred, they are very rare. According to research looking at crimes ending in arrest, violence occurred in only 5% of cases. In most encounters, victims meet offenders voluntarily and expect sexual activity, because they feel love or affection for the person they have been corresponding with. Typically they have sex with the adult on multiple occasions. Most of these crimes are statutory rather than forcible rapes.[2]

➲DO SAY:

Although most victims go voluntarily to meet and have sex with Internet offenders, these are nonetheless serious sex crimes that take advantage of inexperienced and vulnerable young people.

It is important that people not discount the criminality of offenses where the youth participated voluntarily in sex or in initiating or concealing a relationship. Statutory sex crime laws in every state recognize the exploitative imbalance of power and experience that makes relationships between young teens and adults inappropriate. Youth and parents need to know that most Internet sex crimes have this dynamic, so they can accurately identify situations where such crimes may be occurring.

➲DON'T SAY:

Your 10-year-old's "Internet friend" may be a predator.

Virtually all cases of Internet sex crimes involve youth 12 and up.[2] Most victims are ages 13 – 15. Younger children have much less interest than teens in interacting with and going to meet unknown persons they have encountered online. Avoid implying that the typical youngster vulnerable to online offenders is a young child.

➲DO SAY:

Internet offenders target teens who are willing to talk online about sex.

While we need to help parents and younger children prepare for online situations they may confront as they get older, we should not unduly frighten them about criminals who are targeting adolescents rather than young children.

➲DON'T SAY:

Never give out personal information online.

Research has shown that simply posting or sending some personal information online does not put youth at risk.[3] The reason is that most young people (like most adults) do give out personal information. It is hard to be online without doing so. A warning that is so broad and runs counter to such common practices is not likely to make young people trust the source of such advice.

➲DO SAY:

Be careful about who you give personal information to and what kinds of things you share.

Research says that talking about sex online with strangers is a big risk factor for encountering problems.[3] So is interacting indiscriminately with a lot of unknown people online.[4] Youth should be very cautious about how they respond to people who contact them. Other things that probably increase risk are giving out very personal or sexually oriented information, looking for romantic relationships online, and inviting contact from lots of people.[3]

➲DON'T SAY:

Don't have a social networking site or a personal webpage.

Research suggests that personal web pages are not in themselves dangerous.[3] Rather, the danger is when young people use these vehicles to portray themselves as interested in sex, romance, risk-taking, and open to interacting with people they don't know.

➲DO SAY:

Be very careful what you do with social networking sites or personal web pages. It is useful to remind young people that many things they post for their friends may end up being viewed by others, and can prompt contact that could become a problem.

➲DO SAY:

Using the Internet or a cell phone to send sexual pictures of yourself or friends can get you into trouble with the law.

Most youth do not realize that sexual pictures of themselves and other minors can constitute child pornography; its production and transmission are serious crimes. They may see such photos as romantic, fun, adventuresome, or even remunerative. Four percent of youth in the YISS survey said they got requests from online solicitors to take and send sexual pictures of themselves.[1] Youth need to understand why this is a crime, and that people who ask for and transmit such pictures can get arrested as child pornographers and sex offenders.

➲DO SAY:

Don't let friends influence your better judgment when you are online together.

Research suggests youth take more risks when they are online together with other youth.[1]

[3]Wolak J, Finkelhor D, Mitchell K, et al. Online "predators" and their victims: Myths, realities and implications for prevention and treatment. American Psychologist 2008;63 (in press).

[4]Ybarra ML, Mitchell KJ, Wolak J, Finkelhor D. Internet prevention messages: Targeting the right online behaviors? Archives of Pediatric and Adolescent Medicine 2007; 161(2); 138-145.

[Used with Permission from the Crimes Against Children Research Center]

➲DO:

Target prevention education at teenagers in particular.

Research suggests that teenagers are the primary victims of Internet sex crimes and that common teenage vulnerabilities – interest in sex, romance, adventure, independence – are what gets them in trouble.[3] Parents can be helpful, but the research suggests that the most vulnerable youth are ones who are having conflicts with their parents. So we need to reach teenagers directly with messages that are credible. This means not talking down to them; being familiar with their culture; acknowledging their familiarity with the Internet; and respecting their developmentally appropriate aspirations for independence, new relationships and accurate sexual information.

➲DO SAY:

Boys can be criminally victimized online, too.

Research suggests that one quarter of victims of online offenders are boys.[2] Frequently these are boys with sexual orientation issues who get into trouble while looking online for help and understanding they can't get at home or at school. This is a hard topic to talk about openly and sensitively, but parents, educators, youth and law enforcement officials need to understand that youth with sexual orientation issues are a particularly vulnerable group.

The research of the Crimes Against Children Research Center was included in a literature review published by the Internet Safety Technical Task Force led by the Berkman Center at Harvard. Their final report also includes a call for advocates to become more involved in crafting accurate information about Internet risks. Particularly, because the research shows an increased risk for survivors, those of us who work with youth who have previously been victims of sexual abuse should consider talking about online safety with kids and their families before concerns are raised. Additionally, our voices and our knowledge about the reality and dynamics of sexual assault are needed at tables where policymakers, law enforcement and industry are crafting strategies to address Internet risks.

Finally, it is important to bear in mind that youth, regardless of abuse history, explore social interaction and sexual topics both offline and online. Both censorship and restricting access are not viable solutions. Rather, offering information and supporting kids and their families to make informed, savvy choices about Internet use is critical. +

Toby Shulruff supports WCSAP's sister coalitions in the West for the Resource Sharing Project. She has been writing and training on technology safety and capacity in Washington State and nationally since 2001.

TEENS AND SOCIAL NETWORKING

By Grant Stancliff

[*WCSAP: While people of all ages use the Internet and social networking, we know that younger people who have grown up with these technologies have a greater level of fluency. This "language barrier" can present challenges for advocates and prevention staff working with teens. Our work with teens is enhanced when we can increase our understanding of what online social networks are and how they work.*]

MEDIA IS CHANGING. ENTERTAINMENT media like television, video games, and music used to be only a passive medium where viewers consumed without interacting or talking back. Not so anymore, particularly with youth. Many video games are now online and are social experiences that involve interacting with other real people. In many homes, television is either augmented by or replaced by video sites on the web, which facilitate easy sharing and discussion of favorite clips.

Media consumption is becoming inherently social and inherently digital. Technology and the Internet facilitate relationships and community in an organic way for a few simple reasons: things posted online tend to stay there, and can be shared with anyone across the globe. "Sharing" implies a relationship; a relationship implies bidirectional communication. Bidirectional communication, for parents and advocates, means when teens are online, they are essentially in a public sphere with the associated benefits and dangers that carries.

The risk, benefit, and reality of teen Internet usage is of great interest to advocates who seek to prevent perpetration or provide advocacy for survivors. Many teens use the web to access social networking sites. This article will examine the usage habits of teens on these sites. This topic is constantly growing and changing, and so is the language used to describe it. We have included a reference of terms to clarify jargon.

JARGON REFERENCE

• BLOG

The term blog comes from shortening weblog. Blogs are generally designed in a journal format with the most recent item appearing towards the top of the page. A personal blog might have opinions or media a person finds interesting, whereas genre-based blogs have content focused on a particular subject like a product or a position. Blogs often have a place for Comments at the end of a post.

• CHAT

Chatting is any real-time communication with others online. Generally chat rooms are public. Some chat rooms are moderated, and others are not.

• COMMENTS

Blog posts and news articles online usually have an area for feedback from readers. They might be Moderated for safety and appropriateness, and they might not. Social networking sites also allow for users to leave comments on items posted by friends, or on someone's profile.

• INSTANT MESSAGING

Unlike chat rooms, which tend to be public areas, instant messaging is real time communication with a chosen individual from someone's contact list. Instant Messaging software also allows users to see if their contacts are online and what their status is.

• MESSAGE BOARD/FORUMS

Distinct from Comments, message boards are places for people to have discussions on specific topics. Message boards are not real-time, unlike a Chat room or Instant Messaging.

• MICROBLOG

These sites have features similar to social networking sites, but are focused more on sending short messages or updates to every contact at once. These sites were originally designed as companions for mobile phones; they typically employ a character limit. This keeps the content small and fast, encouraging users to follow many people. Security and privacy settings are less robust than social networking sites.

• MODERATED/MODERATION

Moderation is the process by which content is screened for appropriateness. Comments on blogs, and chat rooms are sometimes moderated. Moderation is used for keeping a discussion on topic, or keeping it appropriate for youth.

• SOCIAL NETWORKING SITE (SNS)

Web services that rely on user profiles and information sharing to generate networks and communities. SNSs allow users to be friends with one another, and access each other's content like pictures, videos, notes, or blog posts. They are often used for organizing events, staying in touch, and discovering others with similar interests.

• PRIVATE

Some information posted online is private, and not searchable through a search engine. For example, webmail is posted online, but email is not accessible to others unless security is compromised or it is forwarded to someone who posts it publically. Most social networking sites have security settings to control how private posted information remains.

• PUBLIC

Information that is posted online in a way that can be found by search engines is public information. In general, data files (images, music, documents) are more difficult to search. Nevertheless, if they are posted on a site with some sort of personal information, they are in essence searchable.

• PERMANENCE

When considering risk, it should be assumed that data posted online is permanent. Data backups are made on websites, historical archives are always being made, and people can repost items. Private postings are only slightly less permanent, because those that have access to the private posting can still choose to repost or reuse the content.

For our purposes, social networking sites (SNSs) are not merely sites that have social features. Many websites have social features, like user reviews or the ability to leave comments after an article. The type of services discussed here are websites aimed specifically at building a network of friends and communities that are user-created and user-maintained. SNSs rely on personal data for their services. Users provide personal information for their profile, such as age, location, and interests. User profiles are essentially a homepage: a central location for information on current happenings, a source of contact, and links to other websites you use like YouTube, Twitter, or Flickr. Social networks are not only a web-based résumé or a homepage. SNSs go further by providing the ability to create connections among users, such as allowing users to be "friends." Friends are allowed to post information to each others' profile, and share pictures or video. Information can be shared quickly and easily from one person to all their friends with just a couple of clicks.

There are thousands of SNSs on the web. Many are intended for niche communities. The most popular mainstream SNSs in the United States are MySpace and Facebook. Other social networks, like Bebo or Orkut, are attracting users internationally. All of the above use more or less the same model of profile, friends, and facilitated communication.

One of the larger concerns about SNSs is that they allow harmful strangers access to children and teenagers, and right in our own homes. News stories of such encounters are particularly sensational, and incite wide concern. Dateline NBC's segment To Catch a Predator highlights the number of potential perpetrators and the ease with which they can use the Internet to arrange exploitive and illegal acts. [*For more information see Kids' Online Safety article in this issue.*]

The technology is new. Public responses are also new. Initial prevention efforts are aimed at avoiding the social aspect of the Internet, and in particular, avoiding placing or sending any personal information on or over the Internet. Programs aimed at parents and children have held this as the first rule of online safety. This unplug strategy would absolutely eliminate the concern, but is likely unrealistic with the saturation of Internet usage. Teens are more mobile than younger children. As a result, it is more difficult to restrict their actions. If a home computer is unplugged, they may use a computer at a friend's house or library. Whatever the case, many of them are using social networking sites.

55% **of teens have a profile on a social networking site.**

91% **use the sites to keep in contact friends they see regularly.**

49% **use them to make new friends.**

Pew Internet & American Life Project

TEENS ONLINE

A hidden assumption in the unplug strategy of online safety is that there is little or no value in the kinds of activity that teens use the Internet or SNS for. Using a social site might be viewed by adults as just hanging out at best, and risky at worst.

Researcher danah boyd has done work specifically in this area. In her work, she has found that teens use SNSs for many of the same reasons they do anything social. People are not accidentally social creatures. We find it fun to talk and share, but in doing so, we are defining who we are. Brick by brick, we are defining our individuality. We are sharing culture and ideas. Social networking sites facilitate the same communication—the same thing that might happen over a water cooler, at a coffee shop, or at a table in a mall food court. Of course, there are a few differences between Facebook and a food court table. Namely, it's a lot easier to get to Facebook. There are fewer traditional boundaries like distance, curfews, or a lack of spending money. SNSs are a public space, and they allow teen interaction in a place that is particularly accepting of them. They meet online in digital publics "because their mobility and control over physical space is heavily curtailed and monitored" (boyd, Jenkins, 2006). It is easier to get to and there are not people telling them to move along.

Teens are creating an identity and sharing culture online. While some may post content or blog anonymously, much of the purpose of social networks is to share that information with friends. It is important to note the permanence of such content. Most

content posted online does not go away. In this sense, digital publics raise new challenges: online personas have an extraordinarily long half-life, and every detail is a simple search away. This kind of highly public biography is routine for a celebrity, but unprecedented for most.

The unplug strategy ignores the value of social networks in the lives of teens. The unique aspects of online culture are opportunities to impart teens with new skills about how to manage risks and dangers, while still receiving the benefits of social networks. It is a call to advocates to discover these challenges and create novel solutions. New strategies for safety will have to be developed by advocates and youth to be inclusive of the reasons social networks are used, and the real potential dangers faced online.

Youth are defining many of the ways new technologies are used. As advocates, we are rightly sensitive to the risks. However, we serve our communities best by understanding not only why teens use SNSs, but also what they get out of them. In the process, we can learn a thing or two about how to use this new technology to enhance the work we are doing, and better serve those who are using these technologies. +

Grant Stancliff is the Prevention Specialist at Washington Coalition of Sexual Assault Programs. He presented on Social Networking & Teens at the 2008 WCSAP Conference, and tinkers with ways to use technology for social change.

RESOURCES

Pew Internet & America Life Project
www.pewinternet.org

- "Demographics of Internet Users" November 19 – December 20, 2008 Tracking Survey
- "Daily Internet Activities" Tracking Surveys March 2000 – December 2008
- "55% of adult Americans have home broadband connections" Press Release July 2, 2008
- "Teens and Social Media" December 19, 2007

Bureau of Justice Statistics, "Stalking Victimization in the United States", January 2009
www.ojp.usdoj.gov

National Institute of Justice, "Full Report of the Prevalence, Incidence, and Consequences of Violence Against Women: Findings From the National Violence Against Women Survey", November 2000
www.ncjrs.gov

Internet World Stats, United States of America: "Internet Usage and Broadband Usage Report"
www.internetworldstats.com

2008 Washington Utilities and Trade Commission (WUTC) "Broadband Study Report"
www.wutc.wa.gov

Crimes Against Children Research Center, "Internet Safety Education for Teens: Getting It Right"
www.unh.edu/ccrc

Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States, "Final Report: Enhancing Online Safety"
www.cyber.law.harvard.edu/pubrelease/isttf/

boyd, danah, & Jenkins, Henry, "MySpace and Deleting Online Predators Act (DOPA)"
www.danah.org/papers/MySpaceDOPA.html

For more information:

SafetyNet:
National Safe & Strategic Technology Project
www.nnedv.org/projects/safetynet

National Online Resource Center on Violence Against Women, Special Collection: Technology Safety
www.vawnet.org

Washington Violence Against Women Network
www.wavawnet.org

*For information about becoming a member of **WCSAP,***
*please e-mail us at **wcsap@wcsap.org,** or call **(360) 754-7583.***

Washington Coalition of Sexual Assault Programs

WCSAP
4317 6th Ave SE, Suite 102
Olympia, WA 98503
(360) 754-7583
(360) 709-0305 T-T-Y
(360) 786-8707 FAX

www.wcsap.org