Power & Control Wheel: On Technology & Abuse

This diagram illustrates some ways that abusers can misuse technology within the context of sexual assault, domestic violence, and stalking. Technologies abusers misuse include, but are not limited to, cordless phones, radio scanners, and baby monitors; emails, text messaging, and instant messaging; computers and software applications; the Internet and websites; spyware or other computer monitoring tools; TTY (text telephones), relay services, and other assistive devices; GPS and other location tracking services; cell phones and other handheld computer phones; cameras and other recording equipment; fax machines; and a variety of other surveillance equipment.



Power and Control Wheel: On Technology & Abuse A Guide for Tech Advocates

This is not a stand-alone handout.

This wheel can be used with a variety of audiences and in different settings: from advocacy and criminal justice trainings to counseling and support group settings. The handout is most effective if you take time to discuss the following: (1) how the wheel represents dynamics used by an abuser, (2) scenarios to illustrate specific abuse tactics and dynamics, and (3) definitions of various technical terms referenced in the wheel.

Why a wheel?

The Technology Power and Control Wheel is modeled after the original Power and Control Wheel developed by the Domestic Abuse Intervention Project in Duluth, MN. The Technology Power and Control Wheel is an attempt to provide specific examples of ways technology is used in the context of domestic violence, sexual assault, and stalking.

The wheel helps to illustrate tactics perpetrators use and the dynamics of abuse. The center of the wheel illustrates the abuser's central goal, which is to maintain power and control over the victim. Each spoke of the wheel represents a different tactic that an abuser can use to maintain this power and control. The wheel's rim, which holds everything together, symbolizes the way that an abuser will use physical or sexual violence or the threat of it in order to reinforce the power of the other tactics.

Use examples to illustrate your point.

Abuse occurs in all segments of our population. Abusers customize tactics to target the victim's specific life experiences (e.g. situations, beliefs, culture, identity, economics, etc). When discussing technology abuse, try choosing examples that reflect experiences of a variety of survivors. Here are some examples:

- An abuser hides a cell phone in the victim's car to listen to her or to track her location via GPS.
- After a young man breaks up with his boyfriend, the ex-boyfriend harasses him via email and IM, threatening to "out" him on MySpace.
- An abuser monitors a victim's emails, keeping the victim from telling friends and family about the abuse or from seeking help.
- Abuser figures out a victim's hidden location by Instant Messaging with the victims' children.
 - Abuser uses TTY to impersonate a victim and try to get the court to drop a protection or restraining order.
- Abuser gets a falsified immigration/ID document for the victim, then threatens to tell law enforcement and get the victim arrested or deported

Technical definitions

Identity Theft: When a person uses key pieces of personal information, such as Social Security numbers, to impersonate someone else or manipulate their life (e.g., to harm their reputation or hurt their financial status by creating or altering online bank/credit accounts).

GPS (Global Positioning System): A GPS receiver is a device that uses satellite signals to pinpoint its exact global location. GPS receivers are small and can be easily hidden; they come in most newer-model cell phones.

Blog: Short for Web log, a personal journal posted online that is often publicly accessible.

Instant Messaging (IM): A service that enables someone to "chat" in real time over the Internet with one or more individuals by typing and sending electronic text. Sometimes IM includes real time sound and video transfers.

Spyware: Surveillance software or hardware that enables an unauthorized third party to secretly monitor and gather information about the user's computer use without his or her knowledge or consent, sometimes from a remote location.