

**Webinar: The Use of Technology to Stalk**

**National Indigenous Women's Resource Center  
August 27, 2014**

Stalking resource center

Presented by:

**Michelle M. Garcia**  
Director  
Stalking Resource Center  
National Center for Victims of Crime  
202-467-8700  
mgarcia@nvc.org

Stalking resource center [www.victimsofcrime.org/src](http://www.victimsofcrime.org/src)

**Stalking**  
resource center

**Training**  
**Technical Assistance**  
**Resources**

- Statutes
- Legislative Updates
- Manuals/Guides
- Videos
- Clearinghouse

The Stalking Resource Center is a program of the National Center for Victims of Crime. The mission of the Stalking Resource Center is to enhance the ability of professionals, organizations, and systems to effectively respond to stalking.

The Stalking Resource Center provides training, technical assistance, and resource materials for professionals working with and responding to stalking victims and offenders.

THE NATIONAL CENTER FOR  
**Victims of Crime**

**Overview**

- Stalking definition
- Common technologies used by stalkers
  - Considerations for victim safety
  - Documentation & evidence
- Q & A

**Stalking**

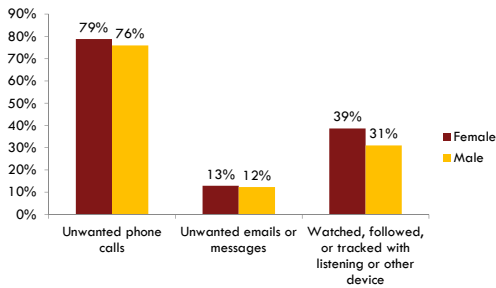
A pattern of behavior directed at a specific person that would cause a reasonable person to feel fear.

**Use of Technology to Stalk**

- Phones – calls, messages, texts, pics, video
- Cameras
- Global Positioning Systems (GPS)
- Computers
- Social networking sites
- Email & IM
- Spyware
- Assistive technologies



## Use of Technology to Stalk



- The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report (2011)

## Technology is Not the Enemy

- ❑ Criminals exploit the technology to create an advantage for themselves
- ❑ Most of the technologies used by stalkers have legitimate and legal functions
- ❑ We must keep up with the criminals and work to enact progressive, inclusive stalking legislation

## Cell Phones

- ❑ Calls, texts, photos, video
- ❑ Cell phone settings can be manipulated to act as listening device
  - ❑ Access to victim
  - ❑ Hidden device
  - ❑ GPS tracking



## Tracking via Cell Phones

## Location Based Services

Search for:

- ❑ Locate
- ❑ Find kids, find friends
- ❑ Track spouse

Find My Friends



GPS Tracking Lite

GPS Phone Tracker

Locate Anyone For Free



FollowMe GPS Tracker

Trackster™ GPS locator



Family Tracker

## Cell Phone Spyware

- ❑ Listen to calls
- ❑ View contact lists
- ❑ Read text messages
- ❑ Activate speaker
- ❑ Locate



## Detecting Cell Phone Spyware

Offender knows things that they could only know if they have access to the phone

Battery overuse and/or high data usage

Offender has or had physical access

Clicks or sounds when on calls

## Call Spoofing

Gives caller ability to change number shown on caller ID, change sound of voice and to record calls.

**SpoofCard** Going to Great Lengths to Hide Your Identity on the Phone?  
BE WHO YOU WANT TO BE



## Major Spoof Providers

Most sites/apps offer 1 free spoofed call

Phonegangster.com



Telespoof.com



Spoofcard.com



SpoofTel.com

## Text Message Spoofing

Send text messages anonymously

- TextEmNow.net
- TextForFree.net



Fake SMS message text

## Considerations for Responders



### Documentation

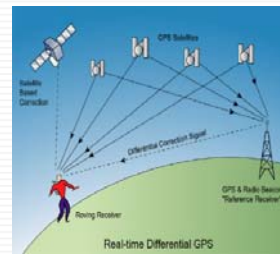
- Preserve audio, SMS (text), MMS (photo, video) on the phone and separate from phone
- Victims can get detailed copies of their own cellphone bills

### Victim Safety

- Educate victims about GPS tracking, spoofing, spyware, etc.
- Option for victims to get new cellphone, but maintain current cellphone



## Global Positioning Systems (GPS) & Locating Devices



## GPS

Active and passive GPS

Small, easily hidden

Map, satellite, bird's eye views

## GPS Documentation & Evidence

1. Locate device on the victim's car
2. Tie suspect to the device

Under Brake Light Cover

Inside Seat Pocket

Under Front Dash

Inside Glove Compartment

Inside Rear or Front Plastic Bumper

Under Seats

Under Vehicle with Magnet

Inside Speaker

Inside Grill (avoid heat)

## GPS Documentation & Evidence

Computer	Phone	Financial Data
<ul style="list-style-type: none"> <li>• Tracking software</li> <li>• Tracking websites</li> </ul>	<ul style="list-style-type: none"> <li>• Apps</li> <li>• Websites</li> <li>• Call-in numbers</li> <li>• Texts</li> </ul>	<ul style="list-style-type: none"> <li>• Equipment purchase</li> <li>• Real time tracking service charge</li> </ul>

## Email

Gmail

Aol Mail

Hotmail

iCloud

YAHOO! MAIL

mail.com

Facebook

Outlook Mail

GMX

## Email

How do stalkers use email?

- Send email
- Monitor email
- Intercept email
- Impersonate victim and send messages to others

## Email Anonymizers

Sites/services that will mask the senders identity

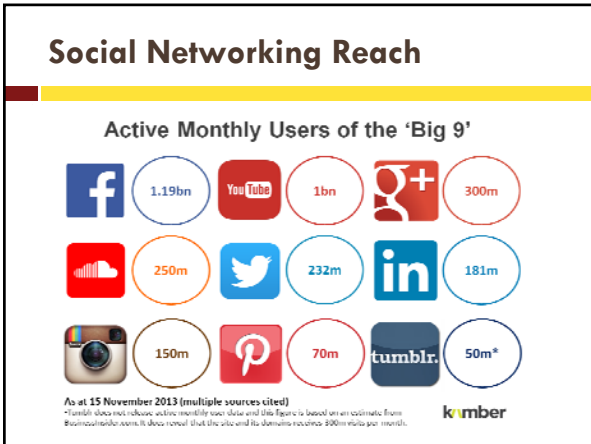
- Email address
- IP address

Hide My Ass

SENDANONYMOUSEMAIL

REVENGE MAIL.COM

## Social Networking Sites



- ### Social Networking Sites
- SNS can bring people together in various ways
  - How stalkers can exploit SNS:
    - Gather information on the victim
      - Location
      - Plans
    - Communicate
      - Post on victim's page
      - Post about the victim on their own or other's pages
    - Create fake sites

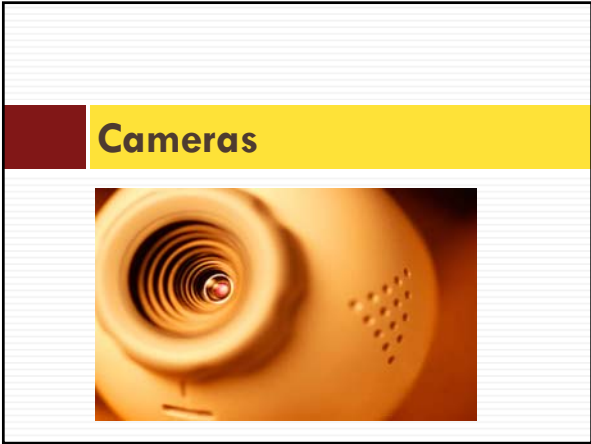
### Considerations for Responders

**Documentation**

- Preserve emails electronically and hard copy with expanded header
- Do not forward emails
- Screen shot social networking posts

**Victim Safety**

- Explore online presence, account security, privacy settings
- Discuss freedom/safety balance
- What is on other people's pages



## How Can They Be Disguised?



## How Cameras are Used

Keep track of victims – learning their routine, monitoring behaviors, etc.

Watch victim without being seen – be omnipresent

Obtain information they otherwise wouldn't be able to have

Manipulate victim; blackmail

Scare and harass— "I'm watching and know what you are doing"

## Camera Considerations



Equipment is inexpensive and easy to access



Look for cameras or common objects in which cameras may be hidden



Camera detection

- Signal detectors
- Lens detectors

## Computers



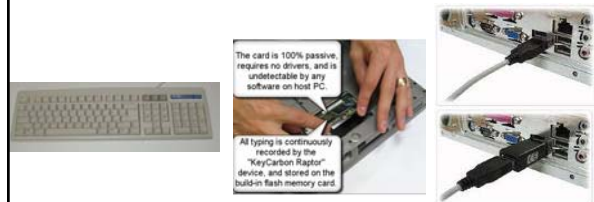
## Computer Spyware

- See everything the victim does on the computer
- Control the functioning of the computer
  - Power
  - Camera
  - Sound
- Can be installed remotely or by physical accessing the computer



## Keystroke Logging Hardware

- Can be keyboard ports, special keyboards, or mouse
- No software to install or configure - just plug it in
- Need physical access to install & remove





## Considerations for Responders



### Documentation

- Commercial spyware detectors (McAfee, Norton, Symantec) may or may not find spyware
- Forensic analysis

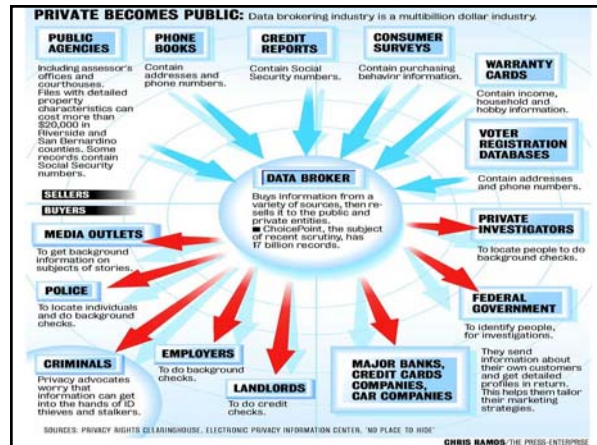
### Victim Safety

- Educate victims about remote access/spyware possibilities
- Encourage victims to use a "safer" computer



## What Information is Out There?

## Data Brokers & Personal Information



## Online Info Considerations



### Victim Safety

- Educate victims about availability of info
- Encourage victims to routinely search for themselves
- Discuss options for having information removed

Any sufficiently advanced technology is indistinguishable from magic.

- Arthur C. Clarke

# Resources

- ## Resources for Law Enforcement
- Regional Information Sharing Systems  
[www.riss.net](http://www.riss.net)
  - Regional Computer Forensics Laboratory  
[www.rcfl.gov](http://www.rcfl.gov)
  - Search  
[www.search.org](http://www.search.org)
  - Justice Technology Information Network  
[www.justnet.org](http://www.justnet.org)
  - Electronic Crime Technology Center of Excellence  
[www.ectcoe.net](http://www.ectcoe.net)



- ## Resources for Victim Service Providers
- For removal of online information
    - Safe Shepherd  
■ [www.safeshepherd.com/advocates](http://www.safeshepherd.com/advocates)
    - Reputation.com  
■ [www.reputation.com/domesticviolence](http://www.reputation.com/domesticviolence)
  - Technology Safety Planning
    - NNEDV SafetyNet Project - [www.nnedv.org](http://www.nnedv.org)

- ## Resources for Victims
- Are You Being Stalked? (Brochure for Victims)
  - Stalking Questions and Answers
  - Stalking Incident Behavior Log
  - Safety Plan Guidelines
  - Cyberstalking: Dangers on the Information Superhighway
  - Ten Things You Should Know About Stalking
- [www.victimsofcrime.org/src](http://www.victimsofcrime.org/src)





# Stalking resource center

## Training

In person training

Webinars

## Technical Assistance

Individual & organizational assistance

Fact sheets, brochures, manuals, guides

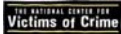
Policy/protocol development & consultation

## Resources

Videos

Online resources

Stalking Awareness Month materials



[www.victimsofcrime.org/src](http://www.victimsofcrime.org/src)

© National Center for Victims of Crime 2014

Content of this presentation may be reproduced for educational purposes with the permission of the Stalking Resource Center.

Please contact the Stalking Resource Center at [src@ncvc.org](mailto:src@ncvc.org) or 202-467-8700 for permission.

This project was supported by Grant No. 2008-TA-AX-K017 awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.