Whatcom COMMUNITY COLLEGE

NCYTE CENTER

PERSONAL DATA VULNERABILITIES

Mark Emry, McNeil High School, Round Rock ISD, Austin, TX

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

Additional materials may be found at www.ncyte.net

PERSONAL DATA VULNERABILITIES

DATA EXTRACTION ACTIVITY

Background Information: When a picture is taken on a smart phone, EXIF (Exchangeable Image File) data is stored as metadata. This data may include location, date, and camera settings. When the image is uploaded to the Internet, that data may be available to anyone. Is yours?

1. Point your browser to pic2map.com
2. Upload the images from the Photos folder associated with this lesson.
3. Collect the data you've extracted in the table below.
4. Note: To keep your images private click the "Keep photos private" checkbox as shown below.

Image Name	Date Taken	Location Data	Other Data Available

CHECK YOUR OWN IMAGES FOR EXIF DATA!

1. Email an image on your phone to yourself using your phone email app.
2. Upload a photo from your phone to pic2map.com and discover any EXIF data on your image. Again, check the box to KEEP PHOTOS PRIVATE.
3. What location (GPS) data is available?

4. When was your photo taken? Find the date and timestamp.
5. What information did you find about the camera?
6. What file data is available?
7. DELETE YOUR PHOTO FROM THE WEBSITE

 This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.