



- Information Security: Accessing CONNECTIONS and Emailing Photos from Smartphones [\(p 1-2\)](#)
- September Computer Training Opportunities [\(p.3\)](#)
- CONNECTIONS Clue: "Tired of Recreating CONNECTIONS Accounts?" [\(p 4\)](#)

## Information Security: Accessing CONNECTIONS and Emailing Photos from Smartphones

The Information Security Office (ISO) has received an increasing number of reports on the use of smartphones or tablets to support casework practice from the field. There is no question about the potential for these devices to not only improve the quality of casework but to increase its efficiency and further streamline business processes. However, as this technology is still in early stages of evolution, the ISO has deemed some practices acceptable and others to compromise integrity and client confidentiality at the present time.

Currently, the ISO has approved the use of smartphones and tablets to access OCFS applications, including CONNECTIONS through the internet, using: <https://connections.ocfs.ny.gov>. It is necessary to first download the Citrix Receiver, or equivalent. Although approved to access CONNECTIONS, there are certain security concerns that must be observed when using smartphones. Some of these, such as the prohibition against storing information on phones, are covered in various documents on the Security page of the [internet](#) and [intranet](#). The remainder of this article will cover one issue in particular, the use of smartphones to store or email case-related photographs.

Using a smartphone or similar device to photograph case-related material and then emailing resulting pictures is very helpful in theory. But in an increasingly sophisticated

### Information Automatically Captured on Your Phone's Images:

1. **Date & Time**—Smartphones and other devices are automatically programmed to record when an image was first captured or last modified.
2. **Location**—Images are almost always geotagged with exact location information, including latitude and longitude coordinates.
3. **Subject**—Advanced software often uses face or object recognition technology to identify image subjects, sometimes by name.
4. **Product**—Metadata goes as far as to indicate what type of device your image was captured on and what specific program was used to capture it.

digital age, this process comes with significant risks to a caseworker's obligation to protect the confidentiality of their clients. Caseworkers may think tasks are being completed more efficiently and that there is a very little chance anyone or anything will notice one little image file traveling through

#### CONNECTIONS INTRANET:

<http://ocfs.state.nyenet/connect>

#### CONNECTIONS INTERNET:

<http://ocfs.ny.gov/connect>

cyberspace. Unfortunately, this is not the case. The CONNECTIONS Implementation team is in the process of developing a mobile CONNECTIONS application that will allow the secure upload of photos from mobile devices directly into CONNECTIONS. However, until this application is implemented, it is important to understand the security risks of emailing mobile photographs and refrain from doing so.

Consider the following fictional scenario that illustrates the process of taking a picture with a smartphone and emailing it to a work-accessible email for inclusion in a case file. Let us suppose that an image is captured of a bruised area of a person's face. The person's name and case ID is in the image's file name, and the image has been sent using a free email utility like Yahoo or Gmail.

Now consider the following:

- ⇒ The image file contains a great deal of *metadata* (data about the file) that includes the precise location of the image—most smartphones or similar devices have a geotag feature, aided by satellite capability, turned 'on' by default. Phones and devices also almost always capture a date and time related to each photograph.
- ⇒ During the email process, the image now resides on a database owned by the company that supports email (i.e. Yahoo or Gmail)
- ⇒ The database is scanned by the company and they employ an increasingly sophisticated array of tools such as: (1) Facial recognition software—which is becoming extremely accurate; (2) Text recognition software that can translate any written aspects of the image; (3) Date and time; and (4) Location
- ⇒ The company that supports the email services may already know that the sender is a caseworker because of links between email and social networking platforms like Facebook or LinkedIn.

As a result, it is completely within the realm of possibility that the child's mother could start receiving email solicitations for local urgent care services, anger management counseling and legal defense services before the emailed file is even opened at the office. Accordingly, the ISO *cannot* currently sanction the use of smartphones to take pictures in support of casework.

The ISO appreciates your patience as the CONNECTIONS team works to implement this new functionality and your observance of the prohibition against sending casework related images using your personal device.

**For more information, or to ask any security-related questions, please contact [ocfs.sm.committee.acceptable-use](mailto:ocfs.sm.committee.acceptable-use)**

### Geotagging at Work on Your iPhone

Want to see how easy it is for mobile devices, like the iPhone, to capture location information? Follow these steps on your iPhone:

1. From the home screen, click on your *Photos* icon.
2. At the bottom of the screen, you should see a *Places* button on the far-right side—click on it.
3. If you have any photos on your device, a map should open with a number of red pins. Each pin indicates where a photo, or a group of photos, on your device was taken. As you zoom in on the map, the red pins will become more detailed, right down to street address.

If this much information is captured visibly on your iPhone, consider the detail of metadata attached to each image that you *can't* as easily see.



## WE'RE ON IT!

*CONNECTIONS Implementation Staff are working to develop a CONNECTIONS mobile application which will allow secure uploads of mobile photographs and similar files directly into CONNECTIONS.*

# September Computer Training Courses



New computer training classes are now available throughout the month of September, in both instructor-led computer labs and via distance-learning options like Training Space and iLinc.

Featured classes include:

- Excel 2010
- Word 2010
- Outlook 2010
- PowerPoint 2010
- Access 2010

More extensive listings of the classroom and distance-learning courses are available on the CONNECTIONS websites at the following links:

**September Online Training**  
([Intranet](#) / [Internet](#))

**September Classroom Training**  
([Intranet](#) / [Internet](#))

Through the  
UAlbany  
Professional  
Development  
Program (PDP), a  
number of useful  
trainings are  
available, dealing  
with both  
standard  
Windows  
programs as well  
as the  
**CONNECTIONS**  
Application

## Need CONNECTIONS Training?

The SUNY Professional Development Program (PDP) provides training on a wide variety of areas within the CONNECTIONS application. Check out the CONNECTIONS Training Page ([intranet/internet](#)) and [STARS](#) for a complete list of offerings.



# CONNECTIONS Clue

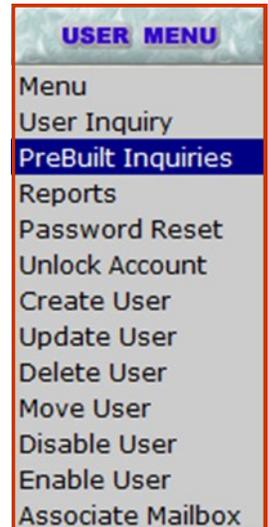
**Are you a Local Security Administrator (LSA) who's tired of recreating CONNECTIONS accounts because your users "forgot" to login often enough?**

**This clue is for you!**

CONNECTIONS passwords must be reset every 90 days. But if the password expires and more than 30 days pass, the underlying HSEN account will be automatically deleted from the Active Directory. There is a small window of time during which the account may still be restored. (LSA's should email [oftsec@its.ny.gov](mailto:oftsec@its.ny.gov) to inquire if this is possible). If this

period of time passes, however, the entire account must be recreated from scratch—a process that requires at least 2 days and a lot of unnecessary work.

But proactive LSA's can shortcut this problem! You can run a report in Webstar that lists passwords that will expire in less than 7 days or less than 30 days or accounts that will be deleted in less than 14 days.



### How?

1. Sign into Webstar with your Administrative account
2. Under the User menu at the top, select "PreBuilt Inquiries"
3. Click the desired report button to generate the report you want
4. Alert your "forgetful" users to login before their account is deleted

## Don't Forget Past CONNECTIONS Clues!

Past CONNECTIONS Clues are available on the CONNECTIONS Website at:

[CONNECTIONS Clues](#) (Intranet)

[CONNECTIONS Clues](#) (Internet)

