Data Security on Mobile Devices

A Higher Education Perspective
July 12, 2011
Background

• FERPA Overview
• FERPA Privacy and Security Requirements
• Securing Mobile Devices
• Examples
• Q&A
FERPA Overview

• **What is FERPA**
  – Family Educational Rights and Privacy Act of 1974
  – A Federal law that protects the privacy of student **education records**. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education
  – FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level
  – Generally, **schools must have written permission from the parent or eligible student in order to release any information from a student's education record**. However, FERPA allows schools to disclose those records, without consent under certain conditions

FERPA Overview

• Directory Information
  – Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them.

So, FERPA Covers…

- Transcripts, exams, papers, graded presentations

- However, FERPA also covers students’…
  - Social Security Numbers
  - State Identification Numbers
  - Drivers License Numbers
  - Discipline Record(s)
FERPA Privacy & Security Requirements

• FERPA does not allow institutions to leave education records unsecured or in a state where access to the records by an unauthorized individual is possible

• This prohibition means that an educational agency or institution must use physical, technological, administrative and other methods, including training, to protect education records in ways that are reasonable and appropriate to the circumstances in which the information or records are maintained

FERPA Privacy & Security Requirements

• FERPA does not mandate any specific method, such as encryption technology, for meeting these standards related to electronic storage and disclosure of information from education records. However, reasonable and appropriate steps consistent with current technological developments should be used to control access to and safeguard the integrity of education records in electronic data storage and transmission, including the use of e-mail, Web sites, and other Internet protocols.

• The integrity and security of data storage and transmission are essential to ensure that information is disclosed only to those who are authorized to receive it.

http://counsel.cua.edu/FERPA/questions/questions2.cfm
FERPA Privacy & Security Requirements

- FERPA does not limit or restrict email as a method for transmitting protected education records. However, it is important to be aware that...
  - Emails specific to an identifiable student are most likely an education record
  - Most emails to students will be identifiable to a student because the email will include the student’s email address or the content/context of the email will be identifiable to a student

http://counsel.cua.edu/FERPA/questions/questions2.cfm
FERPA Privacy & Security Requirements

• Must have written permission from the parent or eligible student in order to release any information from a student's education record.

• FERPA does not allow institutions to leave education records unsecured or in a state where access to the records by an unauthorized individual is possible.

• The integrity and security of data storage and transmission are essential to ensure that information is disclosed only to those who are authorized to receive it.
Securing Mobile Devices (US CERT)

• **Configure mobile devices securely**
  – Auto-lock
  – Enable password protection and require complex passwords
  – Avoid using auto-complete features that remember user names or passwords
  – Ensure that browser security settings are configured appropriately
  – Enable remote wipe
Securing Mobile Devices (US CERT)

• Connect to secure Wi-Fi networks and disable Wi-Fi when not in use
  – Disable features not currently in use such as Bluetooth, infrared, or Wi-Fi
  – Set Bluetooth-enabled devices to non-discoverable to render them invisible to unauthenticated devices
  – Avoid joining unknown Wi-Fi networks
Securing Mobile Devices (US CERT)

• **Update mobile devices frequently. Select the automatic update option if available**
  – Maintain up-to-date software, including operating systems and applications

• **Use appropriate sanitization and disposal procedures for mobile devices**
  – Delete all information stored in a device prior to discarding, exchanging, or donating it
Securing Mobile Devices (US CERT)

- Take appropriate physical security measures to prevent theft or enable recovery of mobile devices
  - For laptops consider using cable locks
  - Use tracing and tracking software
    - Computrace
    - Lookout
    - Mobile Me
  - Never leave your mobile device unattended
  - Report lost or stolen devices immediately
  - Remember to back up data on your mobile device on a regular basis
Securing Mobile Devices (US CERT)

• Use an encryption solution to keep portable data secure. Data protection is essential
  – If confidential data must be accessed or stored using a mobile device, make sure data encryption is enabled or installed
  – Security firms have noted that iPhones and Blackberrys can be used as a secure business tool if the preceding configuration guidelines are followed
iPhone 4 Example
iPhone 4 Example

- Spotlight Search
- **Auto-Lock**: 5 Minutes
- Passcode Lock: On
- Restrictions: Off
- Date & Time
- Keyboard
- International
- Accessibility
iPhone 4 Example

A simple passcode is a 4 digit number.

Voice Dial

iPod Voice Control is always enabled.

Erase Data

Erase all data on this iPhone after 10 failed passcode attempts.

Data protection is enabled.
iPhone 4 Example
iPhone 4 Example
iPhone 4 Example
iPhone 4 Example
iPhone 4 Example
Display a Message
David's T3U

Your message has been sent.
You will receive a confirmation email when the message has been displayed on the device.

OK
iPhone 4 Example
Blackberry Example (v6)
Blackberry Example (v6)
Blackberry Example (v6)
Blackberry Example (v6)
Blackberry Example (v6)
Blackberry Example (v6)
Blackberry Example (v6)
Android Example (Generic)

• Screen Lock
  – home screen > menu > settings > location & security > Set up screen lock and choose between Pattern, Pin or password
In April 2011 Google released new security tools for Android phones:
- Google Apps Device Policy App
  - Locate phone on map
  - Remotely reset password
  - Enabled encryption on Android 3.0
- Remote wipe

There encryption is only an option on:
- Motorola Droid Pro with Update
- Samsung Galaxy S II
Key Takeaways for Securing Mobile Devices

- Only store what you need
- Only store it for as long as it is needed
- Password protect the device
- Encrypt what you store
- Enable remote wipe incase the device is lost or stolen
Data Security on Mobile Devices