Session # 57

Low-Cost Tips to Improve Student Data Security and Privacy

Kristen Lefevre
Ross Hughes
Chuck Tobler
U.S. Department of Education

START HERE GO FURTHER FEDERAL STUDENT AID

An Update on Privacy at the U.S. Department of Education

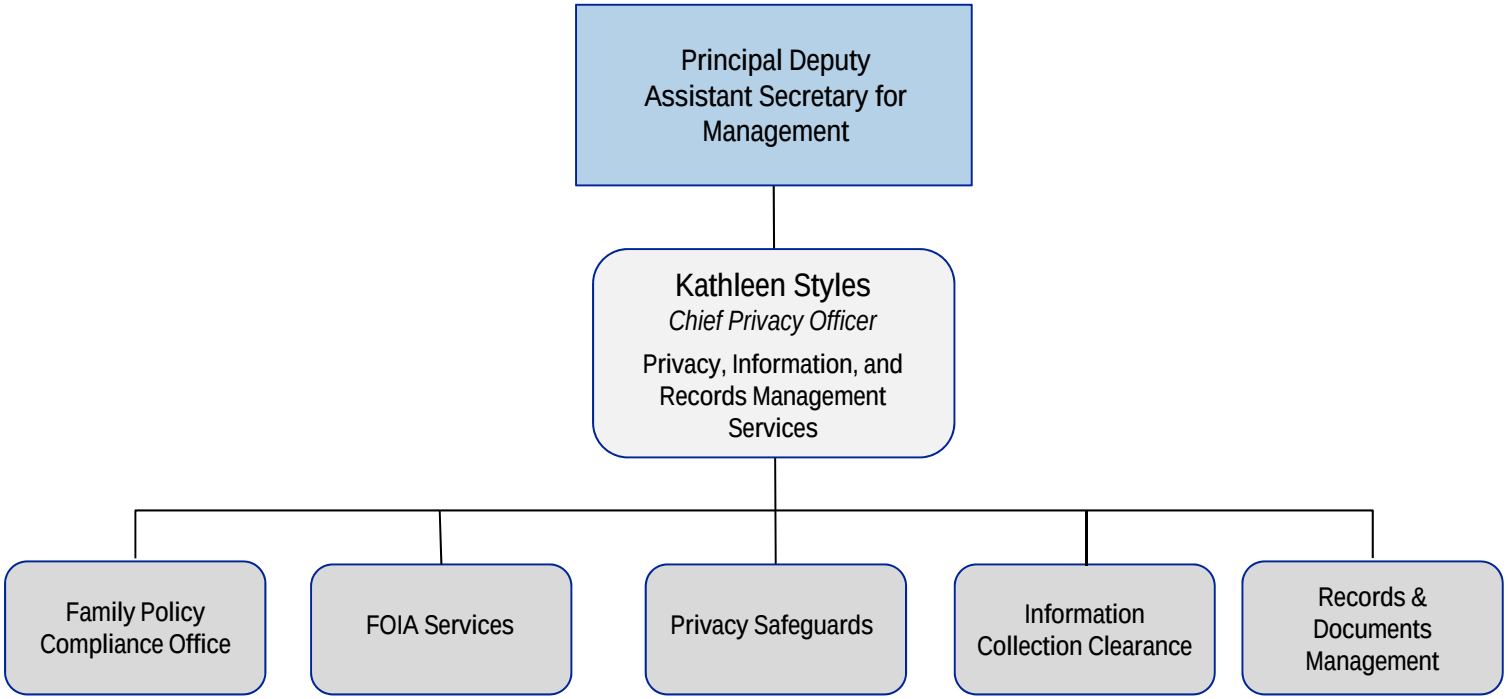
Kristen R. Lefevre
Senior Privacy Specialist
U.S. Department of Education

START HERE
GO FURTHER
FEDERAL STUDENT AID

Privacy Initiatives at ED

- New CPO and Reorganized Privacy, Information, Records Management Services Office
- Privacy Technical Assistance Center
- NCES Technical Briefs
- FERPA Notice of Proposed Rulemaking

Chief Privacy Officer: Organizational Structure



START HERE GO FURTHER FEDERAL STUDENT AID

Privacy Technical Assistance Center (PTAC)

- “One-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices
- Initially focused on longitudinal data systems, but now broader
- Provides technical assistance to states and other education stakeholders
- Disseminates updated information and best practices related to privacy, confidentiality, and security

http://nces.ed.gov/programs/Ptac/Home.aspx

START HERE GO FURTHER FEDERAL STUDENT AID

PTAC, Continued

- "Privacy Toolkit" including best practice guides, FAQs, and documents of interest
- Technical Assistance
- Site Visits
- Training Materials
- Help desk support on data privacy and security questions
- Regional Meetings
- Privacy and security practice presentations

Technical Briefs – The Basics

- Intended to assist states with their development of longitudinal data systems
- Seeking input that can help inform future development of official guidance
- Three are currently available:
  - Basic Concepts and Definitions
  - Data Stewardship
  - Statistical Methods for Data Protection

http://nces.ed.gov/programs/Ptac/Toolkit.aspx?section=Technical%20Briefs

Status of Proposed FERPA Amendments

START HERE GO FURTHER FEDERAL STUDENT AID

Image from Microsoft Clipart Gallery

Privacy Incidents by Educational Institutions

All varieties: hacking, loss of portable device, unintentional, insider breach, etc.

Year	Number of Breaches	Number of Records
2005	64	1,886,841
2006	102	2,016,119
2007	107	791,938
2008	103	1,107,001
2009	71	1,062,275
2010	73	1,588,698
2011 estimated	53	389,008

Source: Privacy Rights Clearinghouse, November 2011

Wrap Up

- Questions or comments?

Privacy is *everybody's* business

BEFORE WE BEGIN . . .

START HERE
GO FURTHER
FEDERAL STUDENT AID

What? A Test *Already?*

- Hey, the test is free!

- But seriously, the test is one of the best low-cost ways to improve your security and privacy, because . . .

First Things First: Know Thyself

- … A self-assessment will identify your strengths and vulnerabilities, which will help focus resources
- And, you don’t have to hire an expensive consultant
- And, you don’t have to give us your scores

So, now I know myself

WHAT NEXT?

START HERE GO FURTHER FEDERAL STUDENT AID

Four Key Principles

1. Establish good governance

1. Know what you know

1. Reduce your exposure

1. Remember: Privacy is more than just the IT department

START HERE GO FURTHER FEDERAL STUDENT AID

Tip 1. Establish Good Governance

- Create policies and procedures for protecting sensitive data
  - Enforce penalties for noncompliance

- Identify a privacy official
  - Make sure privacy has a “seat at the table,” and is not just focused on Information Technology

Establish Good Governance (cont.)

- Develop a training and awareness program
  - Lots of good free stuff available
- Publish rules of behavior
  - Make users sign a “confidentiality agreement”
- Have a breach response plan
  - Roles, responsibilities, timeframes, call trees, alternates

Is there a corollary to “know thyself”?

YES, AND IT IS . . .

START HERE GO FURTHER FEDERAL STUDENT AID

Know What You Know

- Do you know how much personally identifiable information (PII) you have? Where it is stored? Who touches it—and why?
  - Focus on computer systems, also forms, USB drives, CD-ROMS, etc.

- Map out your business process flows—follow the PII trail

Tip 2. Complete a PII Inventory

- An inventory will help you:
  - Identify your critical risk areas
  - Identify opportunities to reduce your collection and use of PII (***the only PII that is truly safe is the PII that is never collected***)
- An inventory of your PII holdings is also the critical first step toward implementing Tip 3

Tip 3. Reduce Your Exposure

- Enforce a clean desk policy
- Conduct PII “amnesty” days (shred paper PII/eliminate PII from local drives/shared drives)
- Protect data at the endpoints
  - USB drives, paper, laptops, smartphones

Reduce Your Exposure (cont.)

- Destroy your data securely
- Do not keep records forever
- Limit access to only those with a need to know
  - Enforce role-based access, least privilege

START HERE GO FURTHER FEDERAL STUDENT AID

Reduce Your Exposure (cont.)

- Practice breach *prevention:*
  - Analyze breaches from other organizations
  - Learn from their mistakes
  - Adjust your policies and procedures accordingly

- Please—THINK before you post/send/tweet!

Is he *ever* going to talk about information technology?

YES

START HERE GO FURTHER FEDERAL STUDENT AID

Last Tip: Privacy Is More Than the IT Department

- People, processes, and technology—all must work together
- Once more—bake privacy in, don't bolt it on (privacy by design)
- Move beyond the "tootsie roll" defense (hard on the outside, soft on the inside)

START HERE GO FURTHER FEDERAL STUDENT AID

Scary Stuff

- One Month's Customer Stats from a Single Vendor
  - 193,989,043 networks attacks blocked
  - 64,742,608 web-born infections prevented
  - 258,090,156 malicious programs detected and neutralized on user computers (Kaspersky Lab)

- 52% of organizations in a recent study said they have experienced an increase in malware attacks as a result of employees' use of social media (Dark Reading)

- 27 of 100 tested Google Chrome extensions have been found vulnerable to data (passwords, history, etc.) extraction attacks on public WiFi networks (Help Net Security)

START HERE GO FURTHER FEDERAL STUDENT AID

More Scary Stuff

- Reports of network security incidents at Federal agencies have soared 650% in the last 5 years—a 39% increase in 2010 alone (USCERT)

- A "brute force" attack on an iPhone can cycle through 9 password guesses per second

(Black Hat 2011)

- Password cracking by security experts:
  - Six characters: 12 seconds
  - Seven characters: 5 minutes
  - Eight characters: 4 hours

(UKFast)

START HERE GO FURTHER FEDERAL STUDENT AID

Some More Scary Stuff

- Headlines:
  - Speedy malware infects more than 6 million Web pages
  - Hackers penetrate website for Nokia developers
  - Hackers steal SSL certificates for CIA, MI6, Mossad
  - Hackers spied on 300,000 Iranians using fake Google certificate
  - Mexican editor's death linked to work with social media
  - Facebook Blind Date Ends in Supermarket Robbery
  - USA Today's Twitter Account Falls Victim To Hackers
  - Ads On Bing, Yahoo Leading To Malware Downloads
  - Twitter Hack Hits Bank Of Melbourne
  - Internet scams harvest billions of dollars

Even More Scary Stuff

150,000
malware samples
SophosLabs analyzed this number every day in the first half of 2011—an increase of almost 60% compared to malware analyzed in 2010.

59%
decline in email use
A recent comScore report shows a whopping 59% decline in the use of email among 12–17 year-olds, and a 34% decline for the 25–34 year-olds. Facebook, text messaging and tweets are now the preferred communication methods for many people.

4.5
A new web threat is detected every 4.5 seconds
SophosLabs saw an average of 19,000 new malicious URLs every day in the first half of 2011– that's one every 4.5 seconds.

1 Million
people duped
The FBI estimates that a cybergang tricked nearly a million people into buying its fraudulent software. With a price point from $50 to $130 (depending on how many "extras" the victim gets talked into), this netted them over $72,000,000.

99.999%
people on the Internet are people you don't know
Remember not to share your information with every "friend" you meet online.

81%
social network security risk
Sophos asked approximately 1,700 computer users which social network they felt posed the biggest security risk and Facebook at 81% "won" by a landslide. A significant rise from the 60% who felt Facebook was the riskiest when we asked the question a year ago.

85%
of organizations have established an acceptable use policy
But only 69% of these organizations have specific policies for company-owned mobile device users. And, this number further decreases when you consider policy for employee-owned mobile devices (31%), reinforcing the need for establishing AUPs for all mobile devices.

68,593,657
people viewed "Chocolate Rain" on YouTube to date
If your friends ask you to view this video on Facebook, do not click. It may be a clickjacking scam.

(Sophos Security Threat Report Mid-Year 2011)

START HERE GO FURTHER FEDERAL STUDENT AID

High Cost of Security

- Homeland Security 2011 budget request is for $614.21 million for cyber security and communications

- In 2010, network security spending grew 11% vs. 2009, to pass $6 billion, and there already appears to be steady growth in 2011.

- Analysts from ABI Research are predicting that network security spending will exceed $10 billion by 2016

(network equipment.net)

START HERE GO FURTHER FEDERAL STUDENT AID

Security on a Budget

- Use What You Have
  - Don't buy just to have the newest
  - Evaluate threats based on adjusting existing defenses
- Leverage Your Knowledge Base
  - Use your existing skills matched to any new purchases
  - Use your CS department's knowledge
- Use Open Source Solutions
  - Security can be equal to commercial products
  - Remember free is never really free
- Re-Purpose Old Hardware
  - Match requirements against what is in your "obsolete" closet
  - Linux is our friend and the gateway to powerful new systems

Save Some More

- Hire Interns Instead of Professionals
  - Supplement your staff for lower level skill requirements
  - Training cost and time will increase
- Review Your Policies
  - Long term savings if processes are expensive
  - Help to instill the “Human Firewall” concept
- Re-Assess Your Threats
  - Perform annual risk assessments because threats change
  - Get rid of the $100 fence for the $10 horse
- Cut Out the Fluff
  - Stop processes that show no ROI
  - “Security by Obscurity”

Find Those Elusive Saving

- Spend Money to Save Money
  - Cheaper to protect than to recover
  - Shop and compare
- Use Public Resources
  - Government, vendors, Internet (grain of salt)
  - Only pay for consulting as last resort
- Consider Outsourcing
  - May save on benefits, training, etc
  - Staying “state of the art” is their job
- Evaluate Your Insurance Options
  - Transfer your risk
  - Umbrella liability insurance

START HERE GO FURTHER FEDERAL STUDENT AID

Hold That Last Nickel

- Security Is Not Just IT
  - Complete system includes people, technology, and operations
  - Don't be penny-wise and pound-foolish
- Security Cost Is Not Just Purchase Price
  - Think of every aspect before you jump at that low price
  - Compare, compare, and compare again
- Improve Security with Training
  - Internal ability to handle own security issues
  - More knowledgeable staff is a more secure staff

(Global Knowledge)

START HERE GO FURTHER FEDERAL STUDENT AID

Stretch Some Dollars

- Passwords
  - Code
    - Start with a fixed component “mybank”
    - Capitalize the fourth character
    - Move the second to the last character to the front
    - Add a chosen number after the second character
    - Add a chosen non-alphanumeric character to the end
    - n1mybAk;
  - Phrase
    - From your favorite song, verse or book and embellish
    - “8 characters and a special character - $W@7d+SM
  - Change often
    - At least every 90 days
    - But not so often that people write them down
- Encryption
  - Winzip
    - AES encryption
  - Open Source
    - Any good product with at least 256 bit encryption

START HERE GO FURTHER FEDERAL STUDENT AID

Squeeze What's Left

- Session Locks
  - Automatic
    - Lock them down so users can't change them
  - Limit time
    - 15 minutes maximum for desktops
    - Application should be based upon unique requirements (batch processing)

- Awareness
  - Posters
    - Keep security on everyone's radar
    - Change often
  - Training
    - You can't fix stupid – people will always be the weakest link
    - Social engineering can only be fought by awareness and preparation
    - Knowledge is power
  - Notices
    - Emails
    - Newsletters

Down To The Last Drop

- Open Source
  - AV/Firewalls
    - Linux
    - Do your research before you try – fake AVs are a major problem
  - Training
    - Vendor Webinars
    - Internet
  - Policies
    - SANs
    - Vendors
- Physical Security
  - Shred bins
    - Locks
    - Make sure you can't pull things out
  - Computers
    - Secure to the desks
    - Keep in a locked room
  - Wiring closets
    - Locked at all times
    - Inspect often for illegal taps

START HERE GO FURTHER FEDERAL STUDENT AID

Conclusions

- Security might entail some costs, but not having security will cost much, much more
- Saving money is about making sound decisions on the right products and processes that provide the best value
- Security is more than the IT department—people, processes, and technology are the key components
- Privacy and security are everyone's responsibilities—a chain is only as strong as its weakest link
- Call Chuck

Free Security/Technology Resources

- http://www.techsupportalert.com/content/probably-best-free-security-list-world.htm?page=31

This is a link to literally dozens of free security technologies, all available for download.

Free Privacy Resources

- **General Privacy Issues**
  - Electronic Privacy Information Center: http://epic.org
  - Privacy Rights Clearinghouse: www.privacyrights.org
  - Center for Democracy & Technology: http://www.cdt.org/

- **Protecting Against Identity Theft**
  - U.S. Postal Service, Postal Inspections Service: https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/mailtheft/IdentityTheft.aspx
  - Federal Trade Commission: http://www.ftc.gov/bcp/edu/microsites/idtheft/
  - Department of Justice: http://www.justice.gov/criminal/fraud/websites/idtheft.html

- **Tips for Protecting PII**
  - http://business.ftc.gov/privacy-and-security/data-security
  - http://www.ftc.gov/bcp/edu/microsites/infosecurity/
  - http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html
  - www.onguardonline.gov

Free Privacy Resources

- **Responding to Breaches of Personally Identifiable Information**
  - Visa: http://usa.visa.com/download/merchants/cisp_responding_to_a_data_breach.pdf
  - Federal Trade Commission: http://www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html

- **Privacy Training**
  - http://nces.ed.gov/programs/ptac/Toolkit.aspx?section=Webinars%20and%20Presentations
  - http://business.ftc.gov/sites/default/files/pdf/bus69-Protecting-Personal-Information-guide-business_0.pdf

- **Lists of Data Breaches (Use These for Analyzing Other Organization's Breaches)**
  - https://www.privacyrights.org/data-breach
  - http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

START HERE GO FURTHER FEDERAL STUDENT AID

Contact Information

We appreciate your feedback & comments.

- E-mail: Kristen.Lefevre@ed.gov
  Charles.Tobler@ed.gov
  Ross.Hughes@ed.gov

START HERE GO FURTHER FEDERAL STUDENT AID