Faculty Engagement to Reduce PII (Personally Identifiable Information) Risk

Christine L Borgman
David G. Kay

Available at: https://works.bepress.com/borgman/408/
Faculty Engagement to Reduce PII* Risk

Christine L. Borgman
Distinguished Professor and Presidential Chair in Information Studies, UCLA
Vice Chair, University of California Committee on Academic Computing and Communications &

David G. Kay
Department of Informatics, UCI
Chair, University of California Committee on Academic Computing and Communications

University of California Cyber Risk Governance Committee
June 26, 2017
*Personally Identifiable Information

https://betanews.com/wp-content/uploads/2015/06/123456_password_sticky_note-600x400.jpg
Represent the Senate in all matters involving the uses and impact of computing and communications technology, and shall advise the President, consistent with Bylaw 40, concerning the acquisition and usage, and support of computing and communications technology and related policy issues at the University either at its own initiative or at the President's request. (Am Feb 2015)
Problem as given

- Data retention and records management - specific focus on “personally identifiable information” (PII)
- What is the most effective way to reach out to faculty to raise awareness of personally identifiable information (PII) that may reside on personal computers and that could pose a risk in the case of a security breach or virus attack?
To err is human, but to really foul things up requires a computer.

- Unknown
Reframing the problem

• UC professional staff use PII in their daily work
• UC professionals rely on IT in their daily work
• PII are at risk if they remain exposed on mobile devices – or any IT device
• How can the capture and retention of PII be minimized?

https://www.lhsfna.org/LHSFNA/assets/File/Risk%20sign.jpg
Faculty Stakes in IT

• Teaching
  – Course management systems, registrar, etc.
  – Online and hybrid courses

• Research
  – Data- and compute-intensive methods
  – Collaborations inside and outside of UC

• Service and administration
  – Internet provision, everywhere
  – Academic personnel, travel, payroll, grants...
Risky behavior or risky systems?

- Records management requires specialized expertise
- Training everyone in RM is infeasible
- How can best practices for records retention and disposal be designed into UC systems?

10 Usability Heuristics for User Interface Design: *Jakob Nielsen* 1995

1. Visibility of system status
2. Match between system and real world
3. User control and freedom
4. Consistency and standards
5. Error prevention
6. Recognition rather than recall
7. Flexibility and efficiency of use
8. Aesthetic and minimalist design
9. Help users recognize, diagnose, recover from errors
10. Help and documentation
1. Visibility of system status

The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.

• Inform users when PII are being captured or stored and the rules that apply.
• Provide details of what is being captured, stored, deleted, encrypted, etc
2. Match between system and the real world

*The system should speak the users' language, with words, phrases, and concepts familiar to the user, rather than system-oriented terms.*

- Avoid complex explanations of record retention cycles and systems issues
- Use simple terminology relevant to the task
  - Student record information
  - Personnel dossiers
  - Patient information

https://aos.iacpublishinglabs.com/question/aq/1400px-788px/examples-risky-behavior_f0e085c57bcaeb38.jpg?domain=cx.aos.ask.com
3. User control and freedom

*Users often choose functions by mistake and need a clearly marked "emergency exit."* Support undo and redo.

- Make records functions easy to undo
- If user captures or stores PII by mistake, provide easy ways to back out

https://connectshore.files.wordpress.com/2013/04/img_136.jpg
4. Consistency and standards

*Users should not have to wonder whether different words, situations, or actions mean the same thing.*

- Provide consistent guidance within and between systems
  - What are PII in this system
  - How, when, why to store PII
  - What records practices apply
5. Error prevention

Even better than good error messages is a careful design which prevents a problem from occurring in the first place.

- Avoid accidental capture or storage of PII
- Warn and alert users when they capture or download PII

6. Recognition rather than recall

Minimize the user's memory load by making objects, actions, and options visible.

• State changes should be obvious
• Make actions with PII readily apparent
• Do not expect users to remember an action, parameter, or command
7. Flexibility and efficiency of use

*Users of a system may vary widely in experience or regularity. Allow users to tailor frequent actions.*

- Most PII systems are used intermittently
- Most users may be “permanent novices”
- Make actions such as encryption easy and obvious
8. Aesthetic and minimalist design

Dialogues should only contain information that is relevant. Extra units of information diminish the relative visibility of important content.

• Employ the KISS principle in PII systems
• Defer unnecessary information to “more” functions
9. Help users recognize, diagnose, and recover from errors

*Express error information in plain language, indicate the problem precisely, suggest a constructive solution.*

- Always provide an easy way out of trouble
- Explain how to recover from PII risks
- **Never**: 4×× Client *Error. 401 Unauthorized.* The request has not been applied because it lacks valid authentication credentials for the target resource. The server ...

10. Help and documentation

Some documentation usually is necessary. Help information should be easy to search, focused on the tasks, and list concrete steps.

- Provide links to further background on PII issues and actions
- Provide information on best practices
- Provide links to university policies

http://home.ubalt.edu/ntsbarsh/Business-stat/opre/RiskBehaviour.GIF
Faculty Ideal PII Scenario

• Systems that are easy to use and secure
  – Student records
  – Faculty dossiers
  – Research data and documentation
  – Administrative work
• Support best practices for records management
• No breaches
Mission-driven IT planning

• Design and deploy IT that serves the teaching, research, and service missions of UC

• Base design principles and practice on
  – Privacy enhancing technologies
  – Security enhancing technologies
  – Accessibility enhancing technologies

• Joint Senate – Administration governance of IT strategy and deployment
10 Usability Heuristics for User Interface Design: Jakob Nielsen 1995

1. Visibility of system status
2. Match between system and real world
3. User control and freedom
4. Consistency and standards
5. Error prevention
6. Recognition rather than recall
7. Flexibility and efficiency of use
8. Aesthetic and minimalist design
9. Help users recognize, diagnose, recover from errors
10. Help and documentation