UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

UNIVERSITY OF ILLINOIS IT PROFESSIONALS FORUM AT URBANA - CHAMPAIGN

Haunted by Hackers?

Not Anymore!

Meet the Privacy Team, Your Digital Ghostbusters

Privacy Team
Office of the CIO – Technology Services
Identity, Privacy, and Cybersecurity

2023 Fall IT Pro Forum

Today’s Topics

- Breaches in the News
- Creating a Culture of Privacy
- Privacy Principles
    - Privacy by Design
- Introducing the Privacy Team
    - What we do/ don’t do
- Privacy Efforts
    - Prevention, not Reaction
- Q & A

MOVEit Vulnerability and Data Extortion Incident

- 2000 organizations, 62M people
- What happened: malware exploited a vulnerability, ransom notes sent to organizations threatening publication of stolen data
- What we learned
- How it could have been prevented

University of Michigan

- Students, applicants, alumni, donors, employees and contractors could be affected by the data breach. The school says social security numbers, driver's licenses, government-issued ID numbers, financial account or payment card numbers, and health information could all be affected.
- The university contained the incident quickly by shutting down the campus network from the internet.

Ransomware attack on Lincoln College

- December 2021 cyber attack locked out admissions activities
- No personal information accessed
- Not fully operable until March 2022
- Closed on May 13, 2022
- Financially unstable after ransomware attack in addition to low enrollment during the Pandemic

So, what can you do?

Step 1: Awareness

Protect Yourself

Data breaches can lead to:

- Identity Theft
- Financial loss
- Reputation Damage
- Loss of Intellectual Property
- Online Vandalism

Actionable Steps You Can Take

- Use strong, unique passphrases
- Use a VPN
- Enable two-factor authentication (2FA)
- Keep your software updated
- Secure your devices
- Be cautious with emails and third-party apps and services
- Monitor your accounts
- Limit the information you share
- Educate yourself – Get in touch with the Cybersecurity Training Team!

But the truth is, you can only do so much. . .

Step 2: Build a Culture of Privacy and Cybersecurity

"…serve society by educating, creating knowledge, and putting knowledge to work on a large scale and with excellence."

https://www.uillinois.edu/about/mission/

Foster innovation and creativity

Be accountable for our actions and exercise responsible stewardship

Be inclusive, treat each other with dignity and respect, and promote citizenship

Aim High

What is a privacy culture?

- Promote responsible data handling
- Respect for personal information
- Compliance with privacy laws and regulations

SHOULD

A privacy culture strengthens legal compliance, contractual agreements, ethics, morality, reputation, and strategic development.

Building Blocks for a Culture of Privacy
Privacy Principles

- Choice/ Consent
- Notice/ Awareness (Transparency)
- Collection and Use Limitation (Purpose Specification)
- Integrity/ Security
- Individual Participation (Enforcement/ Redress)

✓ Support the Autonomy of the Individual

✓ Maximize Individual Participation in Record Keeping Where personally identifiable information (PII) is involved

✓ Balance beneficence to person & society with data use

✓ Minimize privacy harms to all persons

✓ Enable the principled use of data to support innovation in research, health, student success, and operational excellence

Introducing. . . the Privacy Team!

CONSENT

I AGREE. I DO NOT WANT. I ACCEPT. I DO NOT
CONSENT. REMOVE ME FROM YOUR LIST. I
UNDERSTAND. I WANT. ACCEPT ALL COOKIES. I
NO LONGER AGREE. I CONSENT. UNSUBSCRIBE
ME. I DO NOT WANT. I ACCEPT. I DO NOT
CONSENT. I GIVE MY PERMISSION. REMOVE ME
FROM YOUR EMAI
WANT. ACCEPT AL
PREFERENCES. I
CONSENT. I DO NO
FROM YOUR LIST.
ACCEPT ALL COOKI
LONGER AGREE. I
UNSUBSCRIBE. I A
ACCEPT. I DO NO
FROM YOUR LIST.
ACCEPT ALL COOKIE

TRANSPARENCY

THE UNIVERSITY WILL PROCESS YOUR DATA IN THIS WAY. WE DO NOT SELL YOUR
INFORMATION. READ OUR PRIVACY POLICY HERE. MANAGE YOUR PREFERENCES. WE
SHARE YOUR DATA WITH THESE THIRD PARTIES. THESE ARE YOUR RIGHTS. THIS IS
HOW YOUR DATA IS USED. THE UNIVERSITY WILL PROCESS YOUR DATA IN THIS WAY.
WE DO NOT SELL YOUR INFORMATION. READ OUR PRIVACY POLICY HERE. MANAGE
YOUR PREFERENCES. WE SHARE YOUR DATA WITH THESE THIRD PARTIES. THESE

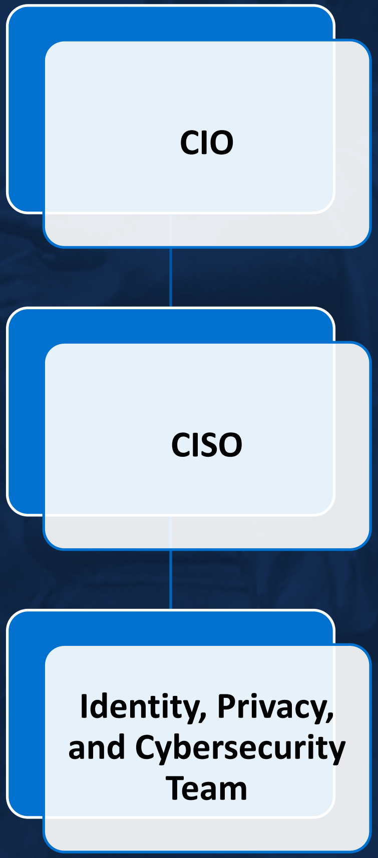
TRUST

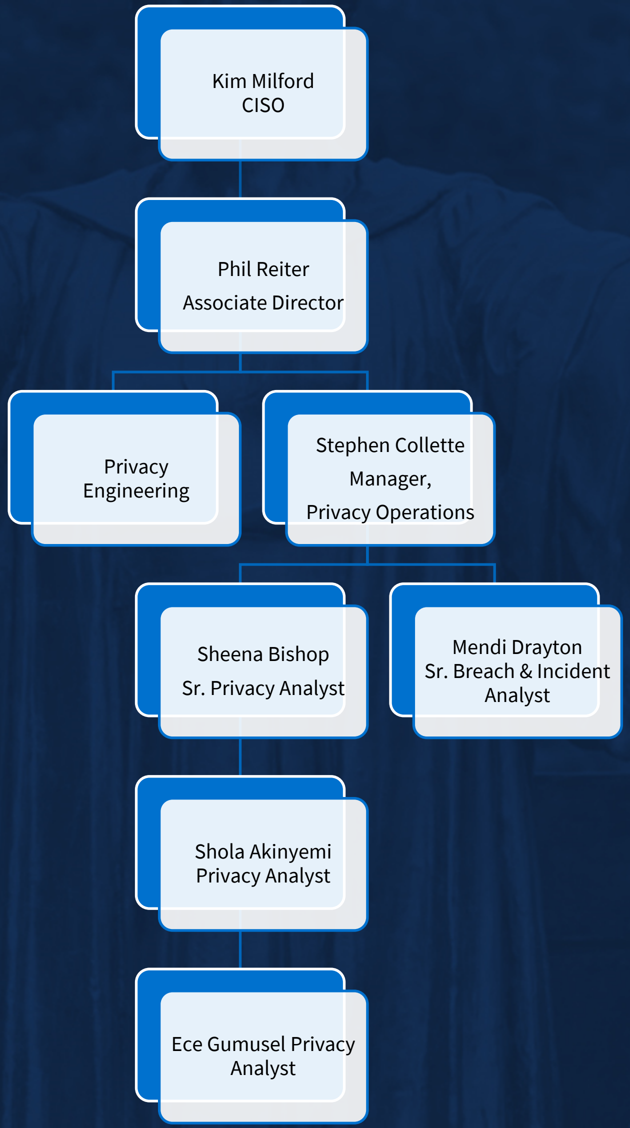
GOOD REPUTATION. I FEEL SAFE. MY DATA
IS KEPT SECURE. PRIVACY-FOCUSED. MY
DATA IS IN GOOD HANDS. I HAVE CONTROL
OVER MY DATA AND HOW IT IS USED. GOOD
REPUTATION. I FEEL SAFE. MY DATA IS
KEPT SECURE. PRIVACY-FOCUSED. MY DATA
HAVE CONTROL OVER
IT IS USED. THE
DATA TO HELP ME
. I GET A SAY IN HOW
OOD REPUTATION. I
S SECURE. PRIVACY-
S IN GOOD HANDS. I
MY DATA AND HOW IT
TATION. MY DATA IS
SAFE. MY DATA IS IN

The Privacy Team of the University of Illinois Urbana-Champaign is relatively new. Our goal is enablement:

- We want our students, alumni, and other data subjects to have a say in how their data is handled, processed, and shared.
- We want our data stewards to be able to do their jobs without sacrificing the personal privacy and personal data of individuals.

Meet the Privacy Team





privacy@illinois.edu

Phil Reiter, Associate Director, Privacy
preiter@illinois.edu

Stephen Collette, Manager, Privacy Operations
sc119@illinois.edu

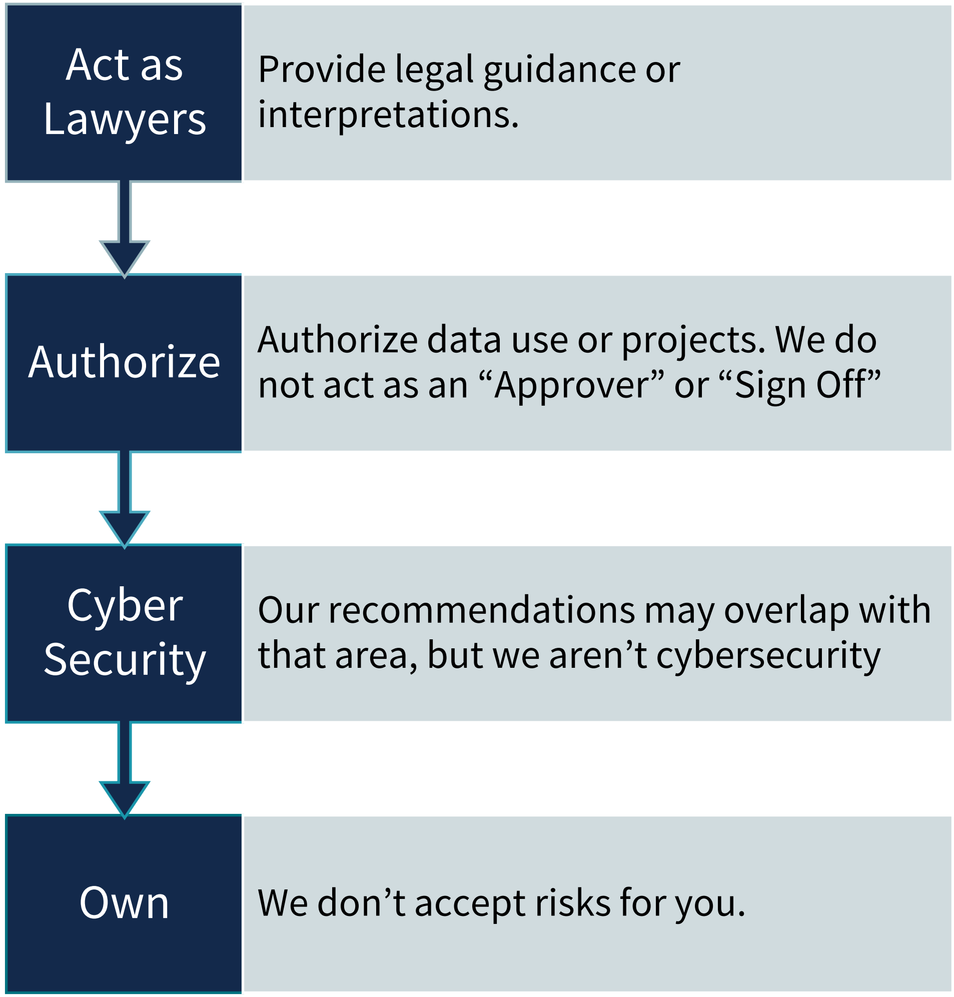
Mendi Drayton, Sr. Breach & Incident Analyst
mendid@illinois.edu

Sheena Bishop, Sr. Privacy Analyst
sheenab@illinois.edu

Oyesola ‘Shola’ Akinyemi, Privacy Analyst
oyesola2@illinois.edu

Ece Gumusel, Privacy Analyst
gumusel2@illinois.edu

What We Don’t Do…



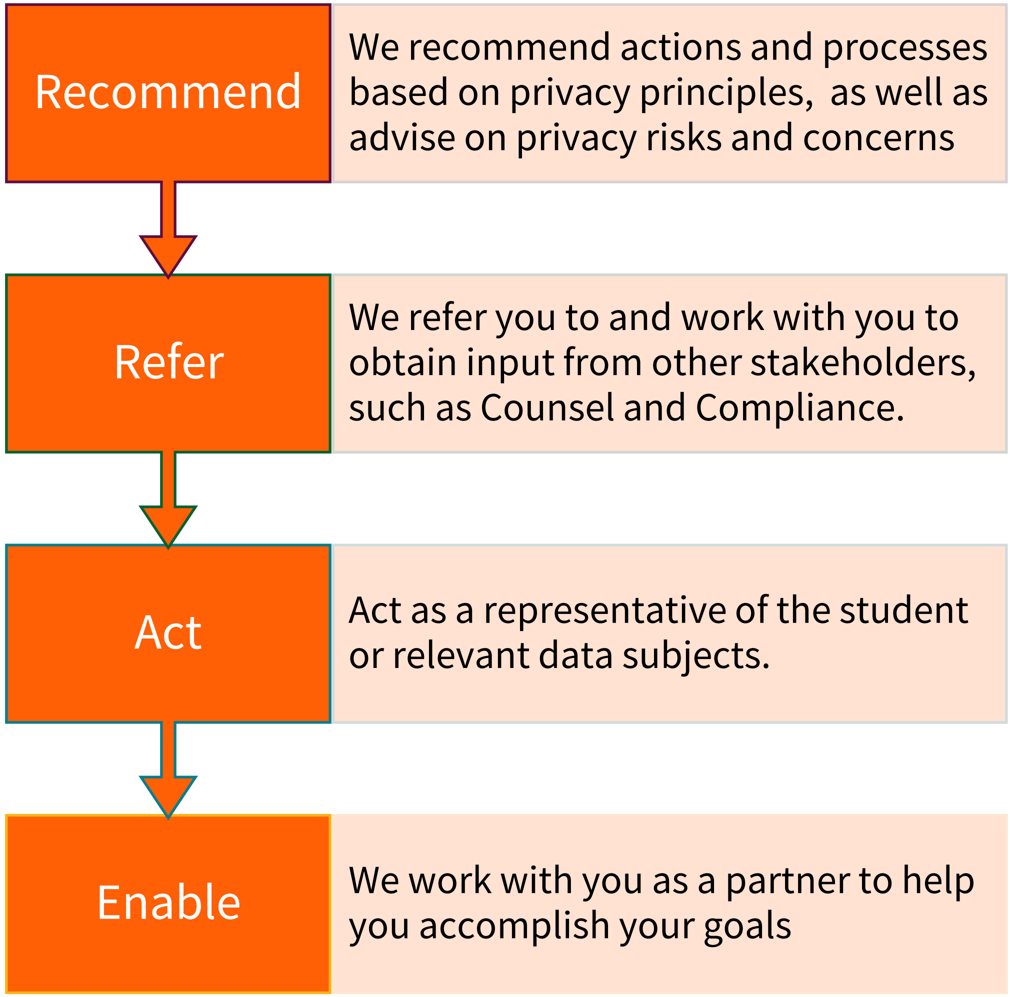
Act as Lawyers – Provide legal guidance or interpretations.

Authorize – Authorize data use or projects. We do not act as an “Approver” or “Sign Off”

Cyber Security – Our recommendations may overlap with that area, but we aren’t cybersecurity

Own – We don’t accept risks for you.

…and What We Will Do



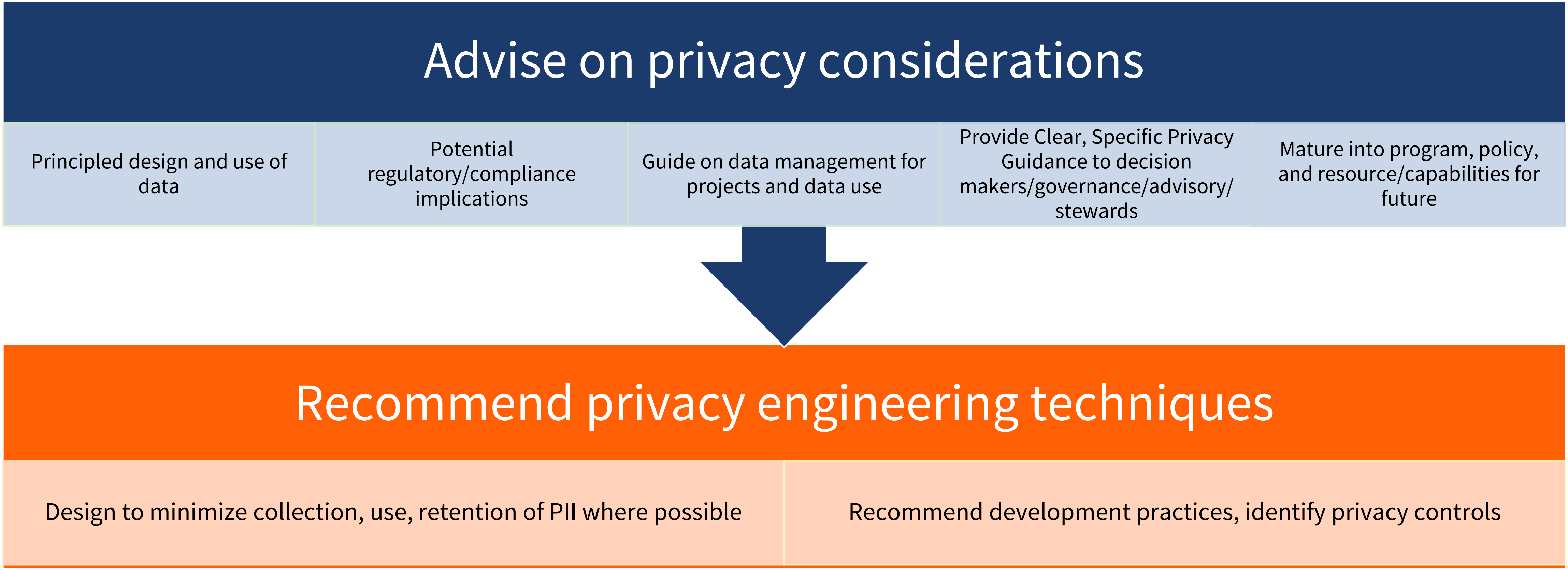
Recommend – We recommend actions and processes based on privacy principles, as well as advise on privacy risks and concerns

Refer – We refer you to and work with you to obtain input from other stakeholders, such as Counsel and Compliance.

Act – Act as a representative of the student or relevant data subjects.

Enable – We work with you as a partner to help you accomplish your goals

Our Process



Advise on privacy considerations

Principled design and use of data

Potential regulatory/compliance implications

Guide on data management for projects and data use

Provide Clear, Specific Privacy Guidance to decision makers/governance/advisory/ stewards

Mature into program, policy, and resource/capabilities for future

Recommend privacy engineering techniques

Design to minimize collection, use, retention of PII where possible

Recommend development practices, identify privacy controls

Privacy Team Support

FREE Consultative Services

- ✓ Privacy Risk/ Privacy Impact Assessments
- ✓ Review of Research Protocol Data, Management Plans, & Data Privacy
- ✓ Data Use and Processing Agreements
- ✓ Contract Review (Data Privacy Protections & Lifecycle)
- ✓ Consent Management
- ✓ Privacy Policy/Practices/Notice Review & Development
- ✓ Illinois Privacy Policy Development
- ✓ Data Governance
- ✓ Data Discovery, Inventory, & Mapping
- ✓ Data Subject Access Request Support
- ✓ Data Breach Incident Response
- ✓ Designs for data minimization
- ✓ Privacy Engineering process designs
- ✓ Identification of privacy controls

Privacy By Design and By Default Mechanisms

Data Minimization

Limit or eliminate collection of personally identifiable information (PII) in data and technology projects

Data Lifecycle

Map use of PII to legitimate processing purpose, collect/store data for minimum purpose and time, and delete

Anonymization

Embed technology capabilities that remove, mask, or escrow direct and indirect identifiers and reduce privacy harms

Federated Learning

Allow research participants and students to share only information needed to gain the value/benefit of a service without giving up sensitive/private information.

Homomorphic Encryption

Process information with PII/sensitive data while the data remains encrypted

Privacy Assessment

DATA CLASSIFICATION

TYPES OF DATA COLLECTED

CROSS-BORDER DATA TRANSFERS

ANALYZE

GUIDANCE

RECOMMENDATIONS

What We are Working on Now

Privacy Center

- A website for students to understand how the university processes their data
  - Includes “privacy profiles” for different types of data, such as “Wi-fi Data” and “Library Data”
  - Helps to translate the University Privacy Statement into layperson terms.

Consent and Preference Management

- A self-service tool for students to manage their data and the consents they have granted the university
- Automation of the management of data subject requests (ex. requests for deletion)

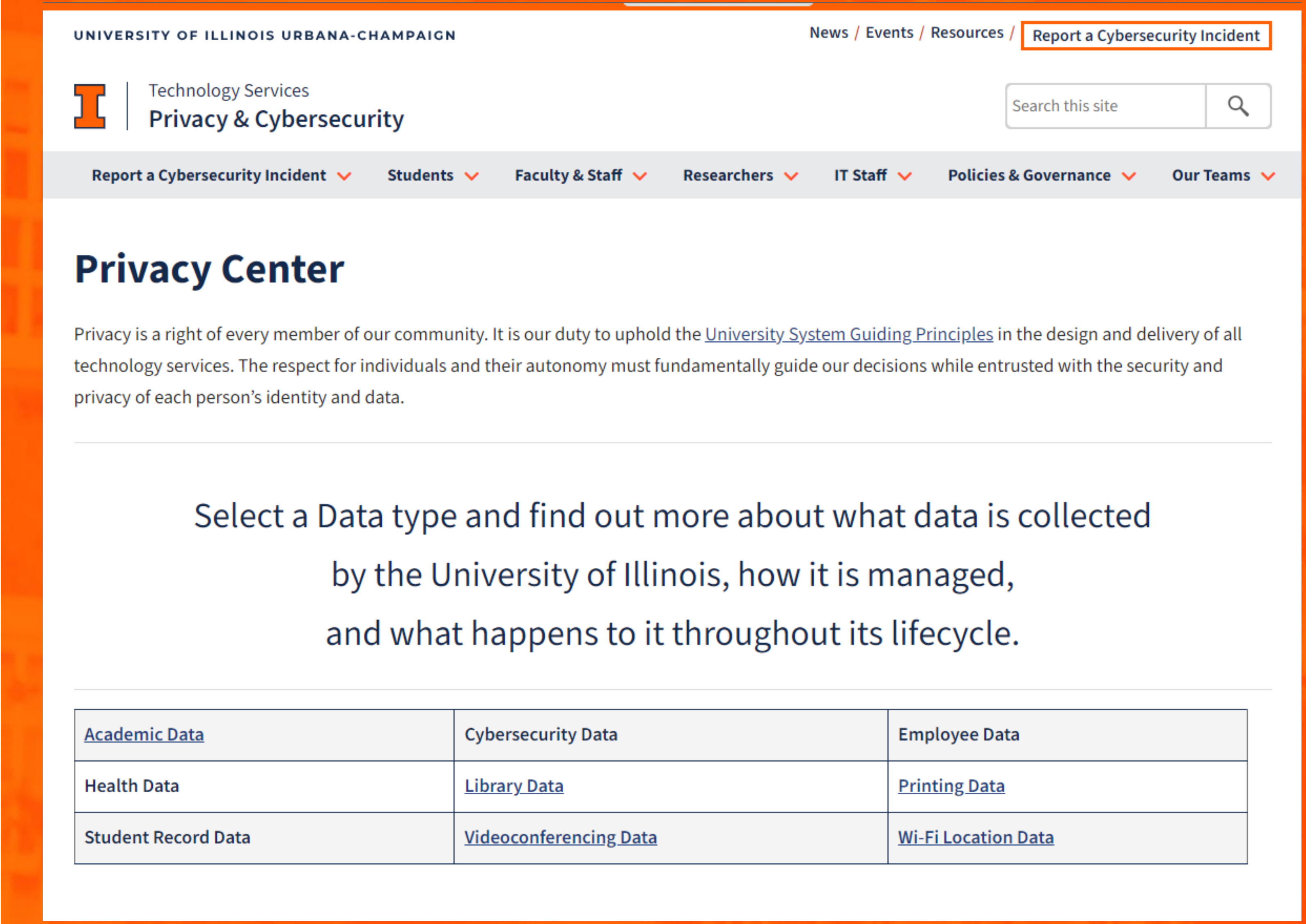
Streamlined review process

- Developing methods to speed up the vendor review process
  - Reducing the number of and/or aligning the assessments & questionnaires requested by different departments
- Automating parts of our engagements to provide immediate feedback to requestors

Maturation of Breach/Incident Response

- The Privacy Team is responsible for the coordination of notifying data subjects in the event of a breach/incident
- Streamlined and documented process to aide Administrative Coordination Team

Illinois Privacy Center

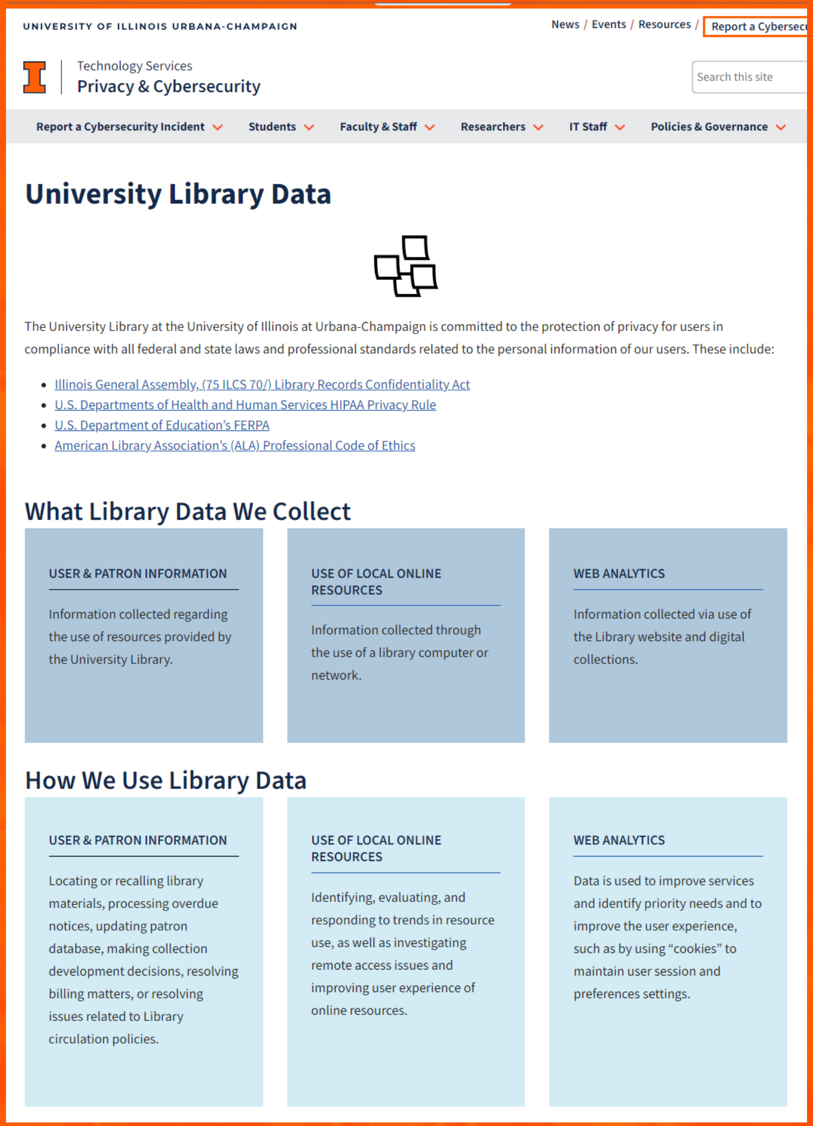


Privacy Center

Privacy is a right of every member of our community. It is our duty to uphold the University System Guiding Principles in the design and delivery of all technology services. The respect for individuals and their autonomy must fundamentally guide our decisions while entrusted with the security and privacy of each person's identity and data.

Select a Data type and find out more about what data is collected by the University of Illinois, how it is managed, and what happens to it throughout its lifecycle.

Academic Data	Cybersecurity Data	Employee Data
Health Data	Library Data	Printing Data
Student Record Data	Videoconferencing Data	Wi-Fi Location Data



University Library Data

The University Library at the University of Illinois at Urbana-Champaign is committed to the protection of privacy for users in compliance with all federal and state laws and professional standards related to the personal information of our users. These include:

- Illinois General Assembly, (75 ILCS 70/) Library Records Confidentiality Act
- U.S. Departments of Health and Human Services HIPAA Privacy Rule
- U.S. Department of Education's FERPA
- American Library Association's (ALA) Professional Code of Ethics

What Library Data We Collect

USER & PATRON INFORMATION

Information collected regarding the use of resources provided by the University Library.

USE OF LOCAL ONLINE RESOURCES

Information collected through the use of a library computer or network.

WEB ANALYTICS

Information collected via use of the Library website and digital collections.

How We Use Library Data

USER & PATRON INFORMATION

Locating or recalling library materials, processing overdue notices, updating patron database, making collection development decisions, resolving billing matters, or resolving issues related to Library circulation policies.

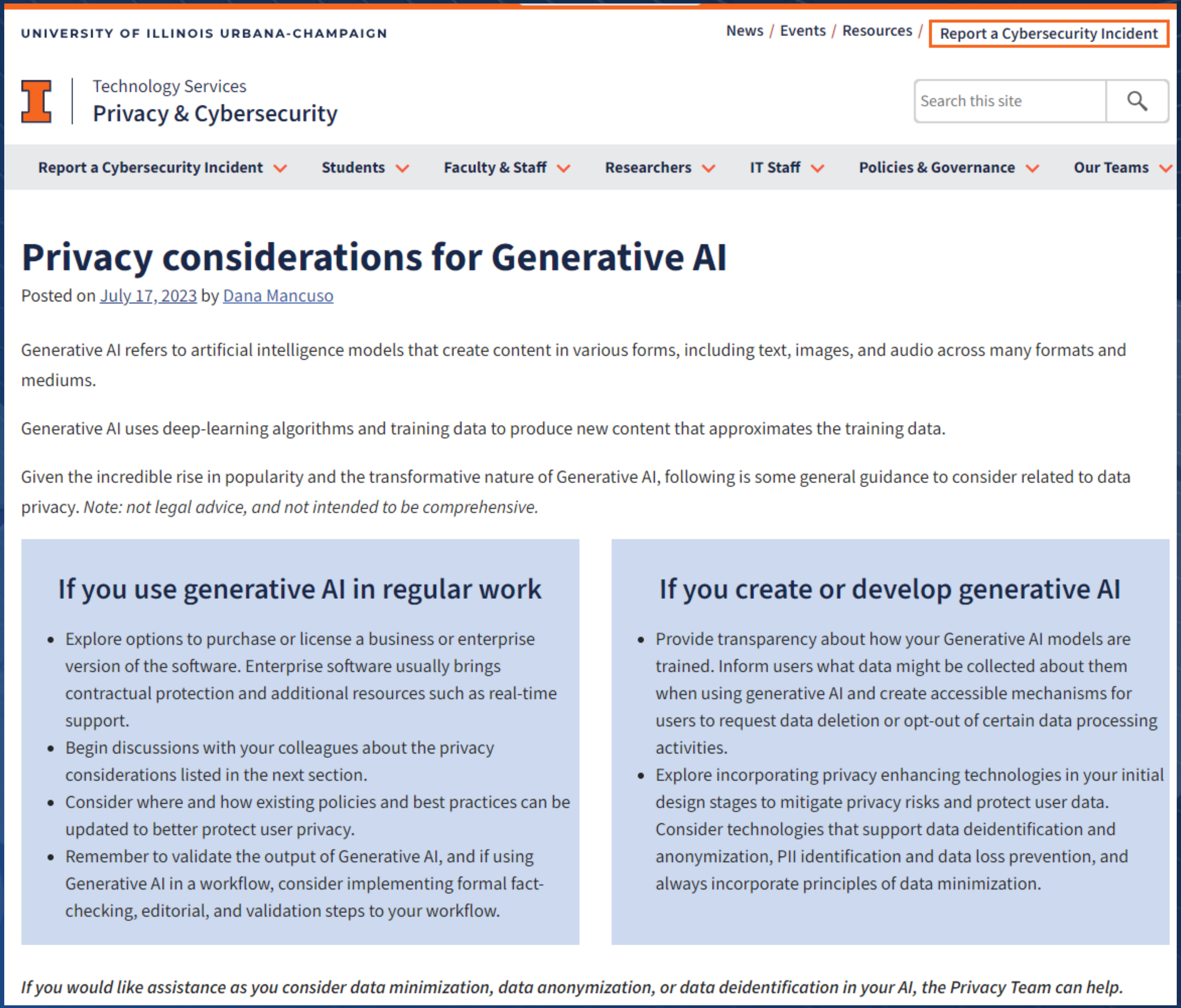
USE OF LOCAL ONLINE RESOURCES

Identifying, evaluating, and responding to trends in resource use, as well as investigating remote access issues and improving user experience of online resources.

WEB ANALYTICS

Data is used to improve services and identify priority needs and to improve the user experience, such as by using “cookies” to maintain user session and preferences settings.

Enabling AI



Privacy considerations for Generative AI

Posted on July 17, 2023 by Dana Mancuso

Generative AI refers to artificial intelligence models that create content in various forms, including text, images, and audio across many formats and mediums.

Generative AI uses deep-learning algorithms and training data to produce new content that approximates the training data.

Given the incredible rise in popularity and the transformative nature of Generative AI, following is some general guidance to consider related to data privacy. *Note: not legal advice, and not intended to be comprehensive.*

If you use generative AI in regular work

- Explore options to purchase or license a business or enterprise version of the software. Enterprise software usually brings contractual protection and additional resources such as real-time support.
- Begin discussions with your colleagues about the privacy considerations listed in the next section.
- Consider where and how existing policies and best practices can be updated to better protect user privacy.
- Remember to validate the output of Generative AI, and if using Generative AI in a workflow, consider implementing formal fact-checking, editorial, and validation steps to your workflow.

If you create or develop generative AI

- Provide transparency about how your Generative AI models are trained. Inform users what data might be collected about them when using generative AI and create accessible mechanisms for users to request data deletion or opt-out of certain data processing activities.
- Explore incorporating privacy enhancing technologies in your initial design stages to mitigate privacy risks and protect user data. Consider technologies that support data deidentification and anonymization, PII identification and data loss prevention, and always incorporate principles of data minimization.

If you would like assistance as you consider data minimization, data anonymization, or data deidentification in your AI, the Privacy Team can help.

What We’ve Also Been Doing

- Actionable recommendations for how the University should handle research on COVID-19 data
- Involvement in large-scale, university-wide and system-wide projects, like Unizin, a data catalog system, email encryption, master contract reviews
- Working on HIPAA compliance reviews for each of our Health Care Components
- Coordinate breach and incident responses with data stewards and other stakeholders
- Created an entire privacy review process for new contracts from scratch…then added to it as we went.
- Guiding the Illinois App team with working towards GDPR compliance
- Partnering with the University of Illinois Police Department on their drone usage policy and procedure
- Reviewing research proposals and provided feedback and recommendations for data privacy considerations
- Developing stronger contractual language for data protection and data privacy
- Developing guidance for generative AI and chatbot usage

Feel better?

Consent
Transparency
Trust

Privacy@illinois.edu

*2024 Privacy Everywhere Conference:
Leading with Privacy
Friday, January 26th, 2023
Beckman Institute & Online