Handling Data With Care: A guide for humans

Heather Hart and Yvonne Lee

April 29, 2025

Arts Datathon: Intelligence

THE HUNTINGTON

Ice Breaker

“What motivated you to join this session?”

Name
Pronouns
Organization
Title

Session Goals

- Understand what PII is
- Learn simple best practices
- Explore how to work with third parties responsibly

Disclaimer

- We are not lawyers
- Even if a law does not specifically apply to you, they can provide a good framework for best practices in data handling
- Please do not record or share any particulars shared in this session without prior express consent from the speaker

What is PII?

- Any data that can be used to **identify a specific individual,** either directly or indirectly
  - Direct: SSN, driver license number, bank account number
  - Indirect: Address, email address, IP address
- The more information you store about a person, the more likely it could be PII when viewed holistically

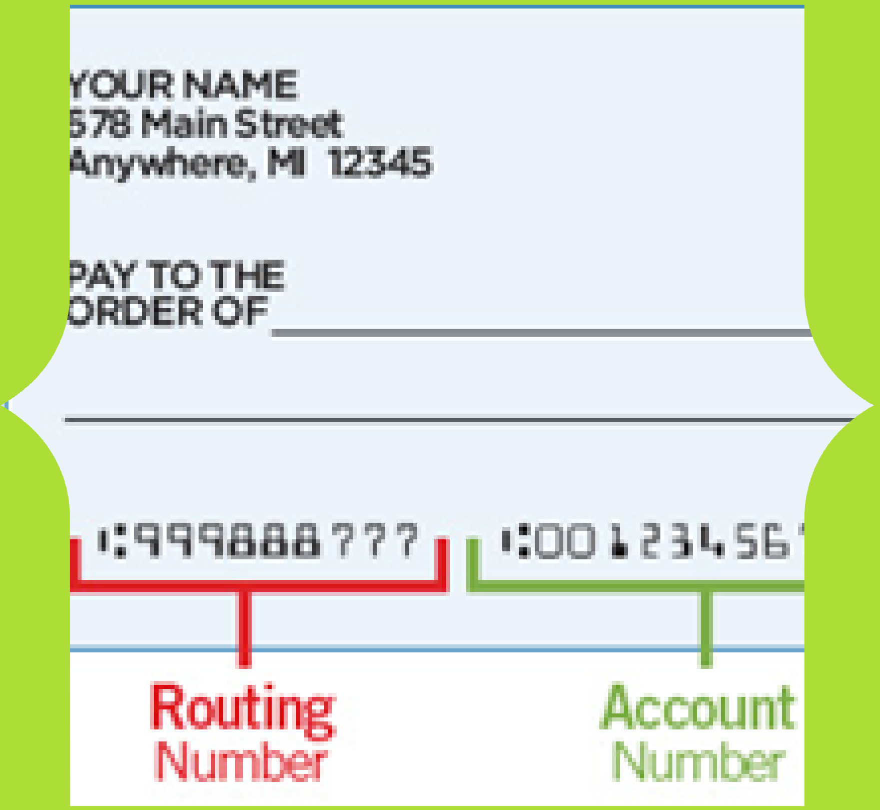
*Not all sensitive or confidential data is PII

Laws Governing PII

- In California, major laws like California Civil Code §1798.81.5, California Consumer Privacy Act (CCPA, 2017), and the California Privacy Rights Act (CPRA, 2020) describe PII
- In California, PII usually refers to first name/initial and last name combined with: SSN, DL, payment numbers, medical info, biometric data, login credentials, postal address
- Under CPRA, sensitive PI includes exact location, demographic data, and data concerning children under 16
- If you have constituents in EU/EEA, GDPR* may be in effect

*GDPR or General Data Protection Regulation is applies to individuals within the EU/EEA regardless of where the org is based

Common Types of PII in Arts Orgs



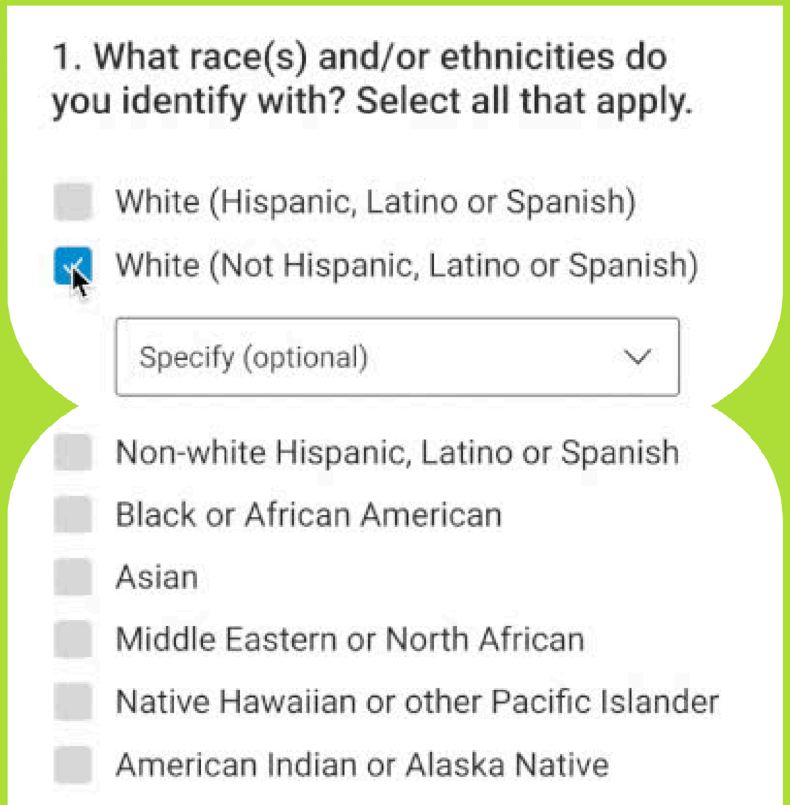
YOUR NAME
578 Main Street
Anywhere, MI 12345

PAY TO THE ORDER OF

⑆999888777 ⑆00123456

Routing Number
Account Number

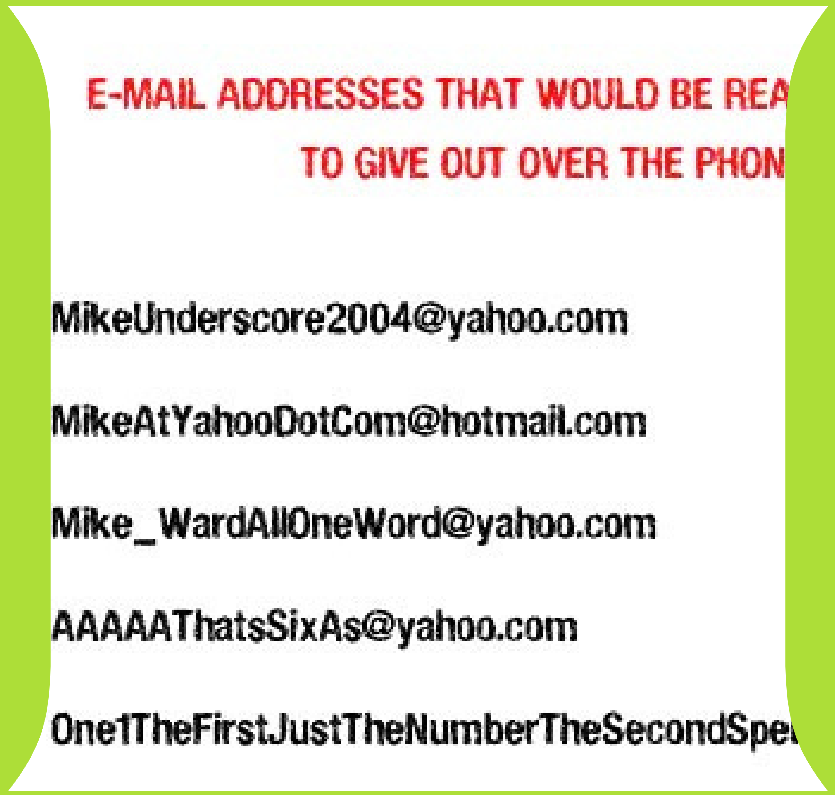
Name
+
Bank Account Number



1. What race(s) and/or ethnicities do you identify with? Select all that apply.

- □ White (Hispanic, Latino or Spanish)
- ☑ White (Not Hispanic, Latino or Spanish)
  - Specify (optional)
- □ Non-white Hispanic, Latino or Spanish
- □ Black or African American
- □ Asian
- □ Middle Eastern or North African
- □ Native Hawaiian or other Pacific Islander
- □ American Indian or Alaska Native

Ethnic Background Survey



E-MAIL ADDRESSES THAT WOULD BE REA
TO GIVE OUT OVER THE PHON

MikeUnderscore2004@yahoo.com

MikeAtYahooDotCom@hotmail.com

Mike_WardAllOneWord@yahoo.com

AAAAAThatsSixAs@yahoo.com

One1TheFirstJustTheNumberTheSecondSpe

Email Address

PII or Not?

Gift Receipts

PII or Not?

Demographic Information

PII or Not?

IP Address or MAC Address

Bonus Question

Dietary Restrictions

Bonus Bonus Question

Nickname

Discussion in Groups

- What type of personal information do you collect?
- Does it rise to the level of PII?
- What are you unsure is PII?

Debrief: PII

“What is the most surprising type of personal info you’ve learned about in this discussion?”

Handle with Care

Transparency

- Privacy policy
- Get consent
- Disclose breaches

Data Minimization

- Essential info only (year or range instead of full birthdates)
- Aggregate when possible
- Retention policy (auto-delete or archive is a standard feature in enterprise apps)

Access Control

Staff Awareness

WWYAOD?

Your Marketing department wants a list of all attendees plus their survey responses from a recent workshop

WWYAOD?

Education needs to share with a grantor all past attendees of school visits

WWYAOD?

Membership wants to send an offer to past visitors to apply admission cost toward a membership

Discussion in Groups

- How do you assess internal requests for data?
- What about external requests?
- How do you mitigate risk if you’re not sure how to proceed?

Debrief: Best Practices

“What is your formal or informal checklist for assessing data collection and sharing requests?”

Working with Vendors

- Only so much possible with OOTB tools
- Contract language matters
- What to look for:
    - How vendors use data
    - How vendors store data
    - Whether they can share it
    - Whether they tell you if there’s a subcontractor
    - Their responsibility if there’s a breach
- Have an Incident Response Plan

Buy Bonds
FREE
PICTURES
FREE
PIC
Your BOND PURCHASES HELP BUY THESE PLANES
Your BOND PURCHAS HELP BUY THESE PLAN
FREE SET OF ckheed Plane Pictures
TH ANY BOND URCHASED AT THIS BOOTH

Contract Language Review

Understand the risks and what your responsibilities are

Contract Language Review

Third party data processors (CRM, email, ticketing) most vulnerable

Contract Language Review

Vendors will (sometimes) change their standard Terms and Conditions if you ask

Contract Language Review

Review language about data protection, access control, breach notification procedures, & insurance limits

Contract Language Review

Ask to see SOC2 or ISO 27001 audit results and check the date

Contract Language Review

Check references and search for past media coverage

Contract Language Review

If you have cyber insurance, your broker may be able to help

Case Study

In 2020, a third-party contractor managing email marketing for the Smithsonian experienced a data breach. SI:

- Issued public statements acknowledging the breach
- Emailed affected individuals
- Reassured members no sensitive financial info was exposed

Discussion in Groups

- What data privacy questions you ask vendors?
- Have you talked about an emergency plan if your data is hacked?

Debrief: Vendors

“What do you regularly look for or ask about in your dealings with vendors and partners?”

Recap

- Keep all staff informed on PII, laws can change frequently
- Minimize data collection, access, and retention
- Trust and public goodwill are everything - be transparent, quick, and empathetic in your communications
- Carefully review vendor contracts and policies
- Have an emergency plan

Resources

- California laws:
  - California Civil Code §1798.81.5
  - California Consumer Privacy Act (CCPA, 2017)
  - California Privacy Rights Act (CPRA, 2020)
  - Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM, 2003)
- California Lawyers for the Arts (https://www.calawyersforthearts.org)
- Center for Democracy and Technology (https://cdt.org)
- Federal Trade Commission (https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business)
- National Council of Nonprofits (https://www.councilofnonprofits.org)
- Nonprofit Risk Management Center (https://nonprofitrisk.org)

Thank You