Meeting the Moment:

Steps Towards Data Minimalism

November 2026

COMMUNITY RESOURCE CENTER

Empowering nonprofits across Colorado to identify and address community needs through connections, convenings, and capacity building.

In partnership with:

Rootable

Scan to learn more about our education offerings.
Contact us at education@crcco.org.

Welcome to Meeting the Moment: *Taking Steps Towards Data Minimalism.* In this conversation, CRC sits down with Lindsey Loberg of Rootable, a cooperatively owned logistics and data platform built by Boulder Food Rescue and partner food-rescue organizations, to talk about how nonprofits collect, store, and use constituent data and why regular audits of these practices and procedures are important across the organization.

"Data can help us serve our missions, and we need to be good stewards of that data." - Lindsey Loberg

Data Security & Data Colonialism Resources (0:00-12:34):

The Costs of Connection **by Nick Couldry & Ulises Mejias:** Defines data colonialism as the appropriation of human life so that data can be continuously extracted from it for profit.

Global Indigenous Data Alliance, CARE Principles: Asks data efforts to consider people and purpose, not just data sharing.

Nonprofit Risk Management Center, How to Secure Private and Confidential Data: Advises limiting collection and limiting internal access to sensitive data.

Data Minimalism Checklist (12:35-27:05):

- First, why are we collecting this information? What are our goals or intentions for collecting this information?
    - Understanding program impact
    - Measure program performance
    - Improving program accessibility
    - Funder reporting requirements
    - *"Just in case" or "It's how we've always done it"*
- Before adding a field to an intake form, database or volunteer, ask:
    - What do we need this information for? Do we have a specific, current use for this data, not a hypothetical future one?

- How will we steward and safeguard this information? Will this data be reviewed, analyzed or acted on within a defined period?
- What are the impacts of this data collection, especially on the people who are sharing their personal information? What are the potential impacts if this data is breached?
- How long do we need to keep this information for? Do we have a data retention policy for this type of information?
- Is this required by a funder or regulator?
- How will this information be monetized? Where are those resources going?
- Can we achieve our ends in different ways?

- **(27:06-39:19)** Run a risk assessment as a team exercise. Consider including staff who set data collection requirements (Directors or development staff), staff who collect personal information from individuals, staff who input datal and staff who interface with people directly and relationally.
  - Consider:

    -Who is being counted, watched, or scrutinized?

    -Who is making money and gaining power from those activities?

    -How are we encountering and implicated in these activities?

Data field	Why we collect it	Who can access it	Risk if breached or misused	Still needed?
e.g., Immigration status	—	—	—	—
e.g., Vehicle / transportation access	—	—	—	—

e.g., Full home address	—	—	—	—
e.g., Race / ethnicity	—	—	—	—

THREAT MODELING WORKSHEET

Fill this worksheet out for yourself or your group. Be honest and realistic. Your threat model can change over time, so revisit it periodically.

Step 1: Identify Your Assets

What do I/we need to protect? (List at least 3)

My private list of contacts

The location of our next meeting

My personal anonymity online

Step 2: Identify Your Adversaries

Who might try to target my/our assets?

Online trolls

Local law enforcement

A counter-protestor group

Based on the civic security guide by github.com/lumpencamp

For each asset, consider the adversaires and what could happen.

Step 3: Assess Risks & Capabilities

Asset	Adversary	What can they do? (Capability)	What is the harm? (Risk)	How likely is it? (Low/ Med./High)
My anonymity	*Online harassers*	*Doxing*	*Threats to my safety, job loss*	*High*
Meeting location	*Counter-protestors*	*Physical surveillance, showing up to disrupt*	*Disruption of event, potential for violence*	*High*

Now that you understand the risks, what cocrete steps will you take to protect your assets?

Step 4: Decide on Mitigations

To protect [Asset 1], I will:_____ *(e.g. Use an ecnrpted message act like Signal and avoid cloud backups of chats)*

To protect [Asset 2], I will:_____ *(e.g. Only share the location one hour before the event via secure channels.)*

To protect [Asset 3], I will:_____ *(e.g. Use a pseudonym online, a VPN, & scrub photos of metadata before posting)*

A PRACTICAL GUIDE TO THREAT MODELING FOR ACTIVISTS

Threat modeling is the process of thinking systematically about what you need to protect and who you need to protect it from. For activists, it's not about paranoia; it's about proactive self-defense. It helps you identify potential threats to your work, your safety, and your community, allowing you to make informed decisions about which security measures are right for you. This guide will walk you through the basic steps to create your own threat model.

CORE CONCEPTS

To build a threat model, you need to answer a few key questions.

01 What are your ASSETS?

Assets are the things you need to protect. They can be digital or physical. Think about what would cause harm if it were exposed, stolen, or destroyed.

- **Your Identity & Anonymity:** Who you are.
- **Your Location:** Where you are, where you live, or where you meet.
- **Your Communications:** Emails, text messages, phone calls.
- **Your Data & Files:** Research, plans, documents, photos.
- **Your Contacts:** The list of people you work with and trust.
- **Your Equipment:** Laptops, phones, cameras.
- **Your Reputation:** Your credibility and public image.

02 Who are your ADVERSARIES?

Adversaries are the individuals or groups who might want to harm your assets. Be realistic about who has the motivation to target you. State Actors: Law enforcement, intelligence agencies.

- **Counter-Protesters or Opposing Groups:** Groups with conflicting goals.
- **Online Harassers & Trolls:** Individuals who attack you online.
- **Malicious Hackers (Black Hats):** Individuals trying to break into your accounts for various reasons.
- **Insiders:** Someone within your group who may not have good intentions.

03 What are their CAPABILITIES?

Capabilities are what your adversaries can realistically do. A random online troll has very different capabilities than a government agency.

- **Online Surveillance:** Monitor social media, read public posts, track connections.
- **Physical Surveillance:** Follow you, watch meeting spots.
- **Technical Attacks**: Phishing (fake emails to steal passwords), hacking into accounts, deploying malware.
- **Legal Action:** Subpoenas, arrests, lawsuits.
- **Information Operations:** Spreading disinformation to damage your reputation.
- **Resource-Intensive Operations:** For state actors, might include mobile phone tracking or obtaining data from tech companies.

04 What are the RISKS?

Risks are the potential negative consequences if an adversary successfully compromises one of your assets. This is where you connect assets to adversaries.

- **Risk:** An online harasser discovers your home address (Asset: Location). **Harm**: Physical danger, intimidation of you or your family.
- **Risk:** Law enforcement reads your unencrypted plans (Asset: Data). **Harm**: Disruption of activities, potential arrests.
- **Risk**: A hacker takes over your social media account (Asset: Reputation/Equipment). **Harm**: Spreading false information, loss of credibility, alienating supporters.

Based on the civic security guide by github.com/lumpencamp

Based on the civic security guide by github.com/lumpencamp

Role of Philanthropy & Data Collection (39:20-46:04):

Remember every field a funder requires is a field the nonprofit has to collect, store, and secure; research shows funders are already moving towards data-minimization.

- The Trust-Based Philanthropy Project says that a more relational approach saves time and gives funders a deeper understanding of the work.
- A 2023 study from Grantmakers in Aging found 90% of funders had streamlined applications or reporting, and 51% had implemented verbal reporting.
- Democracy Fund reported that grantee time on its reporting process fell from an average of 15 hours in 2017 to 5 by 2023.

Creative considerations for philanthropy:

- Use census and local demographic data, instead of requiring individual-level data from grantees.
- Ask process-oriented questions about how an organization is working toward its goals and building its theory of change.
- Do interviews or site visits instead of written reports.

"Data collection can reveal our values. Data is not a replacement for human connection." - Lindsey Loberg

If you are interested in learning more about Community Resource Center's Root Causes Network, click here.

Notes