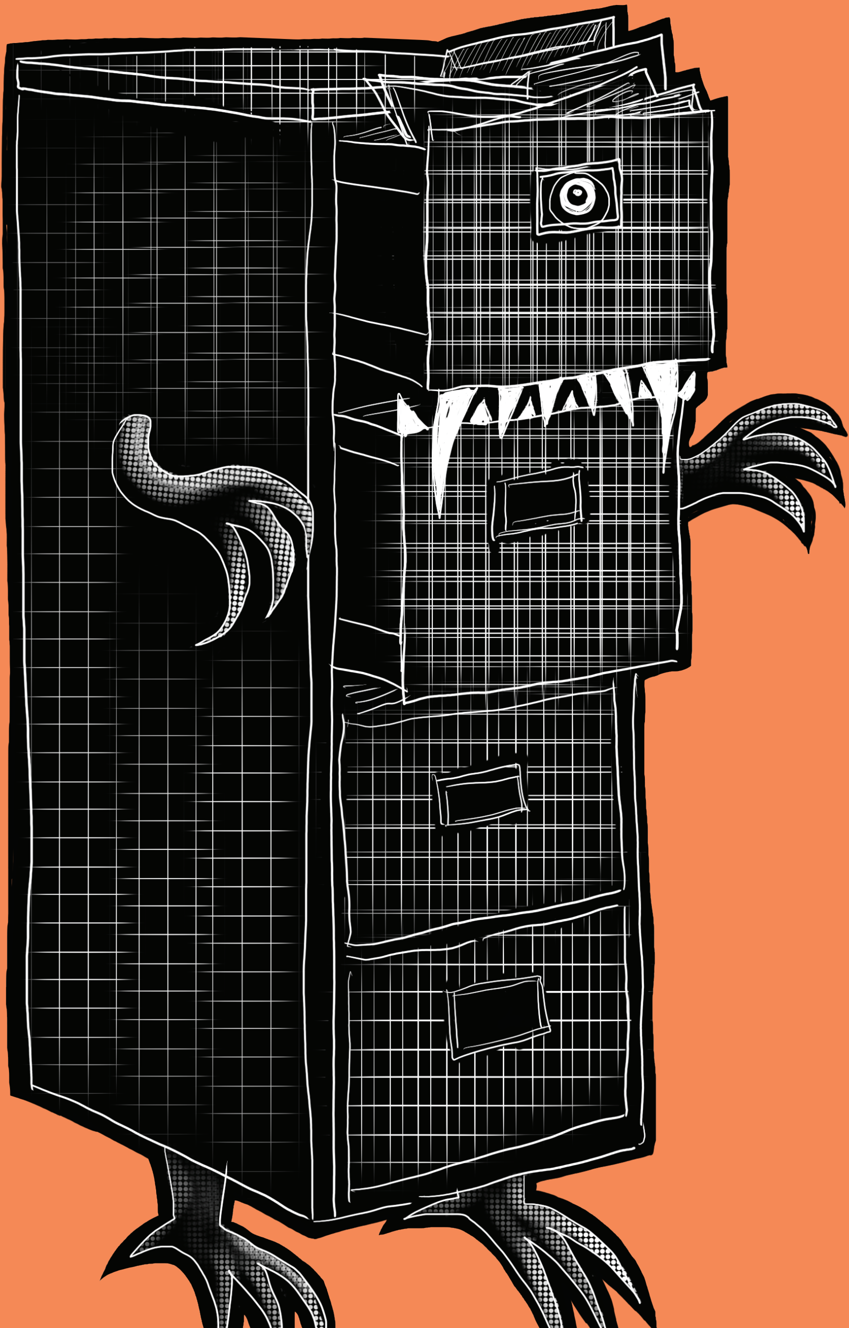
ABOLISH DATA CRIMINALIZATION



CURRICULUM WORKBOOK

Acknowledgements

This curriculum was written by Ana María Rivera-Forastieri, Jamilet Ochoa, and billy dee, in collaboration with Elizabeth Nguyen, Puck Lo, and Pilar Weiss.

We are grateful to the following organizers for providing feedback and insights during the development of this curriculum: Arely Díaz (AMOR), Jennifer Apodaca (Detained Migrant Solidarity Committee), Blanca Pacheco (New Sanctuary Movement Philadelphia), Jamilet Ochoa (Long Beach Immigrant Rights Coalition), and Mario Pérez (Support Don't Deport Collective).

A special thanks to the Inland Empire Immigrant Youth Collective for testing the curriculum and providing critical feedback and perspectives on the issues addressed.

Spanish translation by tilde Language Justice Cooperative.

French translation by Lamia Guellati.

Curriculum design and illustrations by billy dee.

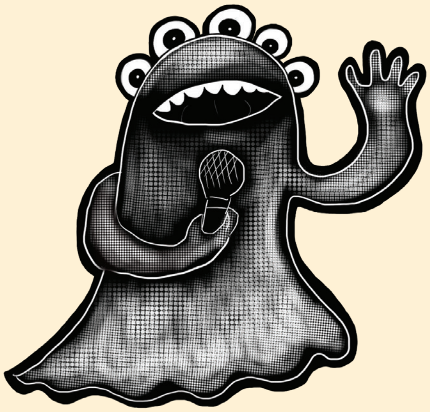
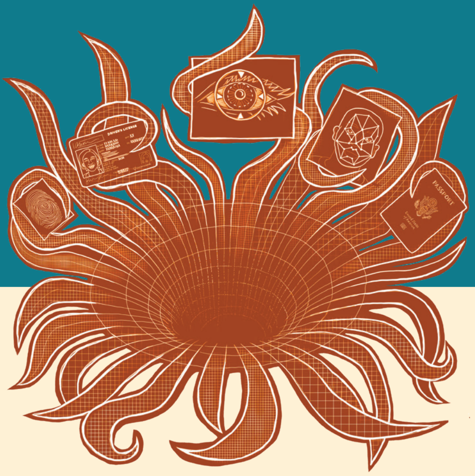
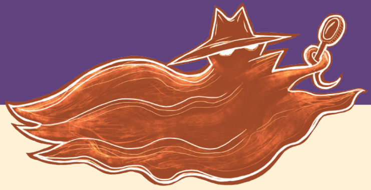


Table of Contents



Introduction



The Abolish Data Criminalization Curriculum Workbook **is an educational tool for organizers committed to learning about and organizing against migrant surveillance and social control.**

In February 2022, Community Justice Exchange launched an interactive website and report titled ***From Data Criminalization to Prison Abolition***. In it we examine and deconstruct some key practices in the surveillance of migrants carried out by both government agencies and private companies to create criminalizing categorizations of people in order to manage vulnerability and exclusion.

We created this curriculum workbook after months of conversations, feedback gathering, meetings with organizers, and workshop testing, to accompany the research we conducted over the previous two years, and to share key concepts and information from the report through a series of guided activities written from a Prison Industrial Complex (PIC) Abolitionist perspective.

This workbook offers guidance for discussions about data criminalization with a focus on lived experiences. We hope that the activities provide space for communities to pause, reflect, and build collective knowledge about surveillance and social control of migrants and criminalized people. Data criminalization impacts many people, including Muslim people and Black people who are not immigrants. This workbook focuses on the use of data to criminalize migrants but we hope that it will be useful to anyone fighting data criminalization. We hope that this resource will supplement existing organizing efforts and inspire resistance and community defense.

Many of us have long fought against the criminalization and deportation of migrants, against tactics of collective punishment, mass surveillance and the triangulation of migrant communities. As it becomes easier for government agencies and private companies to accumulate our personal data, we face unprecedented new threats as we organize against white settler xenophobia and for self-determination.

We are at a crossroads. Because many of DHS' high-tech, interlinked systems still rely on old criminalizing records, and are faulty and incomplete, we believe that the moment to intervene and change course is now.

How do we unmake the multiple machines that create, steal and use against us the very data made from our bodies, daily lives, and connections to other people? We organize!

We're so thrilled to share this curriculum workbook with you!

Workbook Contents & Facilitation Guide

What is in this workbook?

The workbook is composed of five guided activities, a glossary of terms, and an accompanying resources section where you can find selected readings and illustrations. Each activity touches on issues related to data criminalization, surveillance, and social control. The activities also invite participants to imagine ways of resisting and building a world with life-affirming institutions.

How to use this workbook?

This workbook operates as a facilitation guide to activities that will engage participants in discussions, personal and collective reflections, study, and more. Although not required, prior facilitation experience is highly recommended when using this resource. Before planning a workshop, we recommend that you read the entire activity in advance, taking note of any important ideas and suggested conversation topics. We encourage you to adapt or change any of these activities to better suit your community or local context.

The activities were designed as stand-alone workshops for people with varying levels of knowledge and experience. They are not meant to be sequential, but their complexity increases as you progress through the workbook. The suggestions on the following page will help you determine whether the workshop is appropriate for your group.

Deciding if this workshop is right for you:

Activity 1: The Monster Quiz

This activity would be good for groups that:

- Are beginning to understand concepts about data and criminalization
- Learn through individual reflection and conversation
- May or may not already know each other

Activity 2: Where We've Been, Where We're Going

This activity would be good for groups that:

- Are beginning to understand concepts of data and criminalization
- Have experiential knowledge about how surveillance manifests in people's daily lives
- Learn through engagement with images and stories
- Already know each other and have rapport to share personal experiences and opinions

Activity 3: Challenging Information-Sharing Environments

This activity would be good for groups that:

- Have a basic understanding of data and criminalization, and want to understand some of the key concepts outlined in the report
- Want to gain a better understanding of systems and actors involved in these processes
- Learn through reading and discussing ideas
- May or may not already know each other

Activity 4 Unmake the Monster

This activity would be good for groups that:

- Want to focus on how we defend communities in the face of data criminalization
- Learn through acting, play and imagining together
- Already know each other and have rapport to be silly and try out playful energy

Activity 5: Reclaiming Sanctuary

This activity would be good for groups that:

- Have a basic understanding of data and criminalization, and experience and/or knowledge of organizing around these issues
- Want to focus on the practical implications of data criminalization on organizing strategies
- Learn through reading and discussing ideas
- May or may not already know each other

While these workshops are designed to be stand-alone, they can be combined and used in larger settings for expanded learning (e.g. a series of workshops or as part of a convening). We are committed to seeing this resource used by a wide range of organizations and formations, and we would be delighted to provide technical assistance to organizers who wish to use it.

For additional support, please contact us at **info@communityjusticeexchange.org**.

Activity 1:
The Monster Quiz

Workshop Description

This is a guided activity to accompany the Monster Quiz on our website, which was developed as an educational tool to help organizers understand how the machinery of data criminalization uses and shares information collected through different encounters (with law enforcement, during travel, and during day-to-day life activities–like getting a driver's license) to use it against people. Begin by providing an overview of the activity to participants:

- We will take a quiz together to learn about what kind of personal information is collected and stored by DHS databases.
- After we take the quiz, we will have a discussion about how to dismantle the oppressive systems that underpin data criminalization.
- We'll wrap up the activity by articulating values that life-affirming institutions would uphold as opposed to death-making institutions.

Group Size:
15 People

Workshop Length:
1 h 40 min
(longer if more people)

Materials:
In person:
Large sheets of paper, markers, copies of illustration

In Person & Virtual:
Online Access to Quiz

Key Terms:
Data
Data Criminalization
Surveillance

Workshop Schedule

10 min	Welcome, icebreaker, community agreements, reviewing goals
25 min	Introduction: How does Surveillance and Data Criminalization Infiltrate Our Daily Lives?
25 min	Discussion: Data Collection and Criminalizing Potential
10 min	Break
25 min	Visioning: Imagining a Parallel Universe of Data Liberation
5 min	Closing

Introduction: How does Surveillance and Data Criminalization Infiltrate Our Daily Lives? 25 min

Start the activity by having participants take the Monster Quiz. Participants can take the quiz individually or in small groups. Let the group know that they do not have to reveal personal information on the quiz (i.e. they can answer from their own experience or pick answers at random). Encourage participants to look at both the "yes" and "no" answers.

After participants have completed the quiz, take time to understand how they are feeling. Participants may be feeling surprised and disillusioned. They may also feel that the results of the quiz suggest that these systems of data criminalization are operating perfectly and are inescapable. Invite discussion using the prompts below:

- ★ "What is the first word that comes to mind at this moment?"
- ★ "How many of you were surprised by your results?"
- ★ "Did you think this much surveillance was taking place in our day-to-day lives?"

Facilitation Tip:
You can modify this activity by asking for volunteers (or pre-selecting them) to read the questions and answers to the quiz aloud either in the large or small group. If you choose this format, allow for extra time because the quiz will take a little longer to complete.

Additionally, we recommend that you allocate time to go over any definitions or concepts that participants may be unfamiliar with. These can be found in the Glossary of Terms and in our report.

Discussion: Data Collection and Criminalizing Potential 25 min

In this section, we want participants to dive a little deeper into the criminalizing potential of data collection and sharing. Ask the group to start by reflecting on the instances of data collection and potential criminalization (e.g. access to state services, travel, application for immigration benefits, etc.) that we saw in the quiz.

- ★ "From the quiz, what are some examples where data collection and sharing could be used for criminalization?"
- ★ "What were some similarities between these instances?"
- ★ "Can you think about other examples of criminalizing potential that you have encountered?"
- ★ "What are the values and systems that uphold our reality where data criminalization is normalized?"

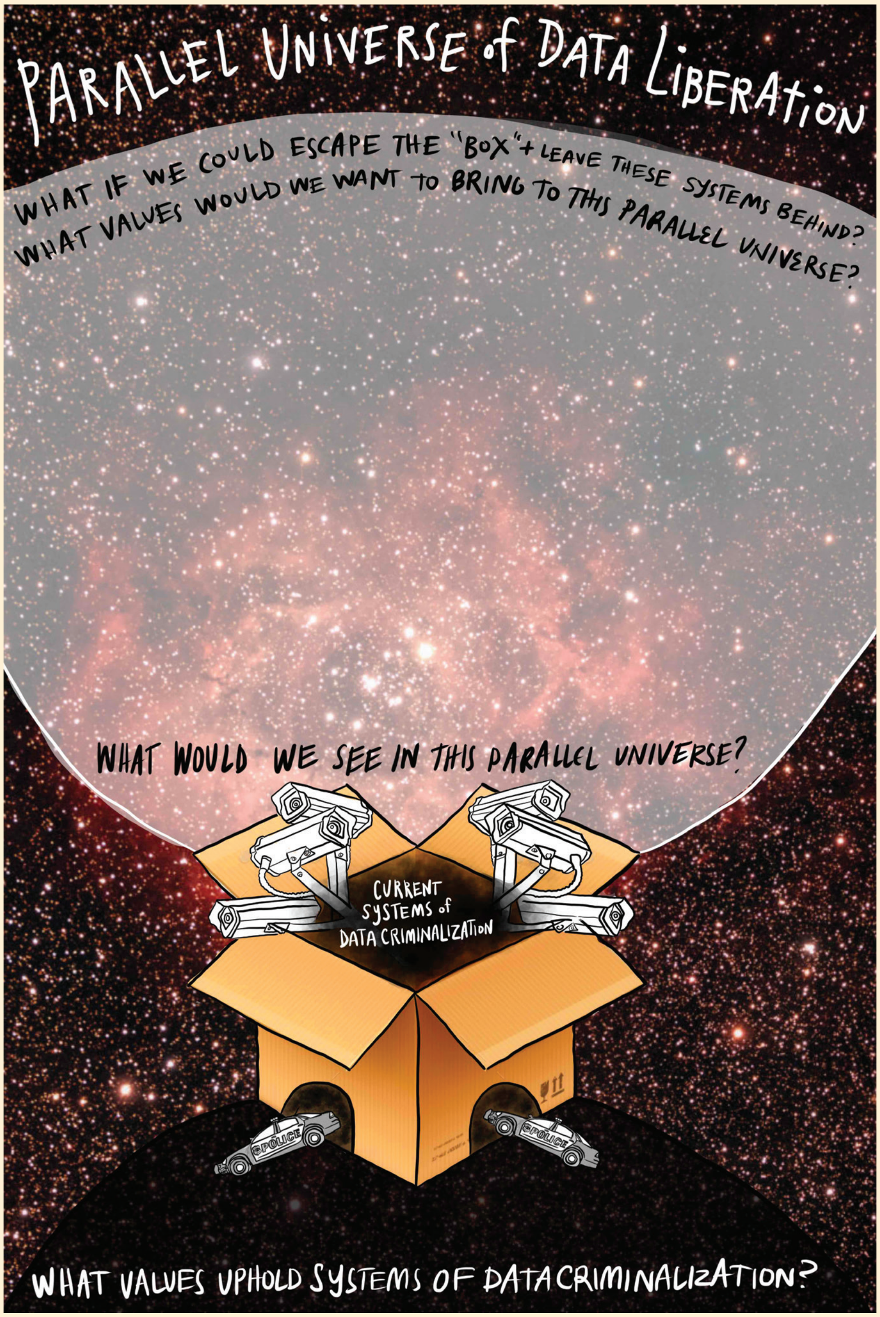
Facilitation Tip:
Ask for a volunteer to take notes on a large sheet of paper (or slide).

Visioning: Imagining a Parallel Universe of Data Liberation 25 min

Invite participants to spend time imagining a "parallel universe" free of surveillance and criminalization. Allow 5-10 minutes for the group to write and/or draw what they would like to see in this parallel universe of data liberation. Ask people to be specific and remind them that using stick figures is completely acceptable for this exercise; there is no need for art "expertise" here, just creativity!

Below are prompts you can use to guide the writing and drawing exercise:

- ★ "Think back to the instances of criminalizing potential you encountered in the previous section, what would be different in this parallel universe?"
- ★ "What are the values and systems that a universe free from data criminalization and surveillance would uphold?"
- ★ "When you wake up in the morning, what would be different about what you see and experience?"
- ★ "What changes would you see in your neighborhood, family, community?"
- ★ "How would the world around you be different? Which institutions would remain? Which would be totally transformed?"


PARALLEL UNIVERSE of DATA LIBERATION
WHAT IF WE COULD ESCAPE THE "BOX" + LEAVE THESE SYSTEMS BEHIND?
WHAT VALUES WOULD WE WANT TO BRING TO THIS PARALLEL UNIVERSE?
WHAT WOULD WE SEE IN THIS PARALLEL UNIVERSE?
CURRENT SYSTEMS of DATA CRIMINALIZATION
POLICE
POLICE
WHAT VALUES UPHOLD SYSTEMS OF DATA CRIMINALIZATION?

Facilitation Tip:

For in-person workshops, give participants paper to write/draw on, and invite a share-out at the end of this section. Alternatively, provide post-it notes that the group can write/draw on and invite them to add their post-it to a large shared paper entitled "Parallel Universe of Data Liberation."

Online workshops may find that a shared "jamboard," or a "padlet" may be ideal for this exercise.

Closing 5 min

Make space for participants to share any final reflections on the quiz or the "parallel universe of data liberation" exercise.

Activity 2: Where We've Been Where We're Going

Workshop Description

This activity is a guided conversation that introduces the concepts of data criminalization and data liberation through illustrations, definitions, and experiential knowledge. Begin by providing an overview of the activity to participants:

- We will start the workshop by looking at an image together that has different elements that show how data is used to criminalize migrants and how it is frequently created through surveillance.
- After we look at the image, we will engage in an exercise to develop an understanding of the concepts of data criminalization and data liberation.
- We will wrap up the activity by exploring some forms of resistance that people have taken or considered on the path to freedom.

Group Size:
15 -20 People

Workshop Length:
1 h 45 min
(longer if more people)

Materials:
In person:
Large sheets of paper, markers, copies of illustration

In Person & Virtual:
Access to Selected Reading and Illustration

Key Terms:
Data Criminalization
Surveillance
Data Liberation

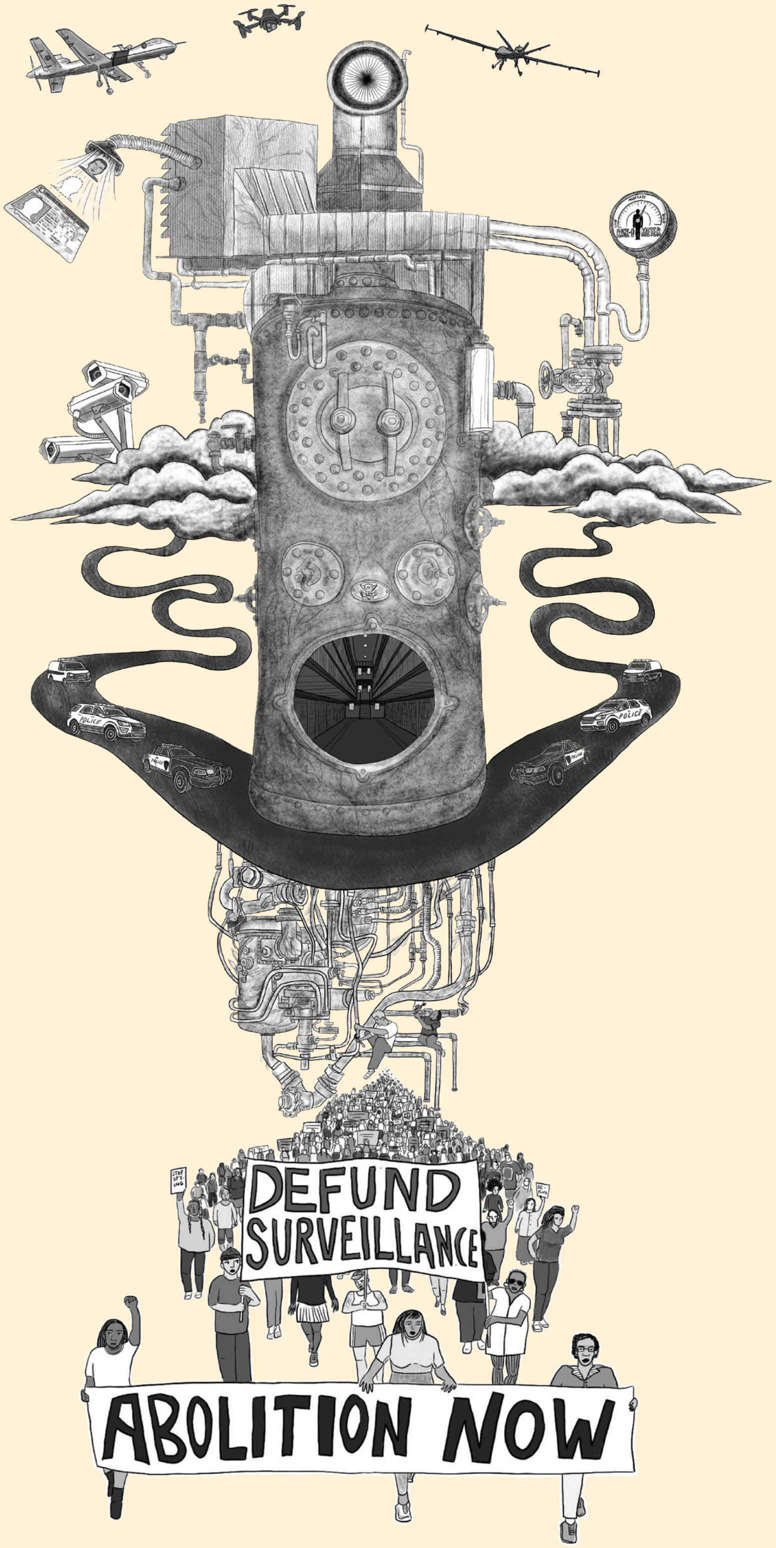
Workshop Schedule

10 min	Welcome, icebreaker, community agreements, reviewing goals
25 min	Introduction: Reviewing the Machinery of Data Criminalization
15 min	Break
20 min	Discussion: Understanding Data Criminalization
20 min	Visioning: How do we fight back against data criminalization?
15 min	Closing

Introduction: Review of the Machine of Data Criminalization 25 min

Let participants know that we are going to take time to look together at an image of the Machinery of Data Criminalization shown on the next page. You can use some of the prompts below as a starting point to guide discussion. Throughout this introductory exercise, encourage dialogue by drawing connections between people's stories and experiential knowledge. Take note of this as people speak and affirm the connections that bring us together.

- ★ "What is going on in this picture?"
- ★ "What systems do you think the police and unmarked vehicles represent? What other actors can we see represented in this machine?"
- ★ "Where do you see surveillance happening in this picture?"
- ★ "What kind of information is being extracted by this machine?"
- ★ "Have you or members of your community interacted with any parts of this machinery?"



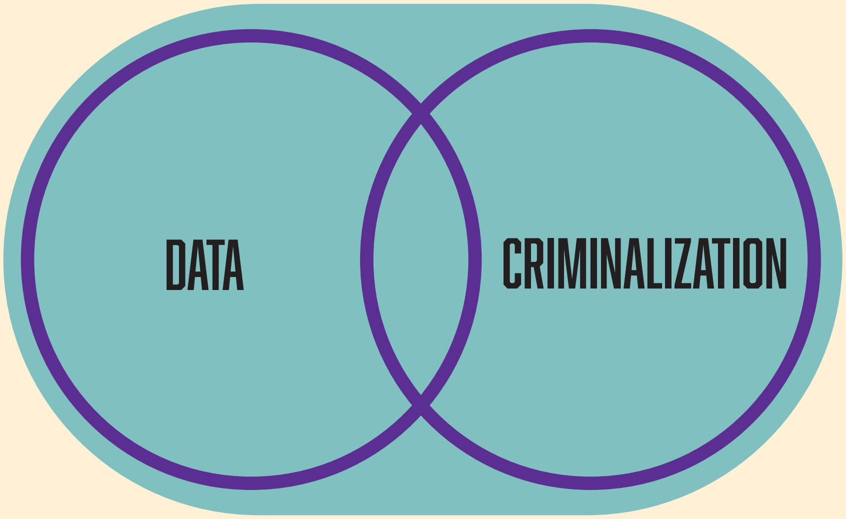
Facilitation Tip:

For in person meetings, we recommend that you print the image on a large sheet of paper, and/or share print-outs of the image with the group and invite participants to write or draw on the copies during this section.

For virtual meetings, we recommend that you screen share an image of the machine and you share a link to it with participants so they can look at the elements more closely.

Discussion: Understanding Data Criminalization **20 min**

In this section, we're going to focus on understanding the concept of data criminalization. Depending on the size of the group, this can be done in pairs, small groups, or the whole group. Create a venn diagram of "Data" and "Criminalization" on a large sheet or paper or shared online jamboard. Use the prompts below to open discussion about these concepts and fill in the diagram.



- "What comes to mind when you think about data?"
- "What do you think about when you think about criminalization?"
- "What do you think happens when these two get combined?"

Facilitation Tip:

Write the definition of any concepts you are reviewing and take notes on a large sheet of paper (or shared slide) so the group can follow along. You may decide that it is best for your group to break down the definitions even further. For example, before beginning the venn diagram exercise, you could spend some extra time discussing the definitions of "data" and "criminalization" separately.

Read the definition of "data criminalization" aloud and take time to define any unfamiliar words or concepts in the definition. Draw connections between the definition and examples shared in the previous section. Invite discussion with the prompts below:

- "What stood out to you about this definition?"
- "Based on this definition, can we think of real-life examples of how data is used to criminalize people?"

Facilitation Tip:

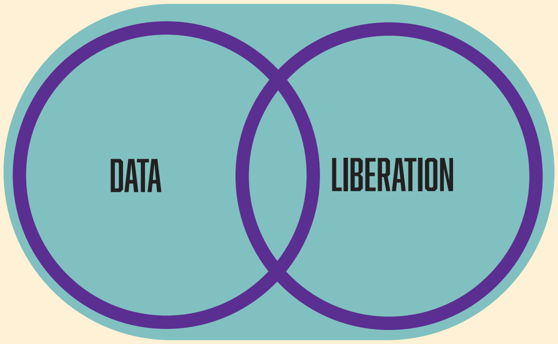
For examples of real-life data criminalization that can be used in the discussion, visit the resources accompanying the report.

Visioning: How do we fight back against data criminalization? 10 min

Resisting may seem impossible in a datafied world where it appears that constant tracking is baked into our daily lives. But people have been finding ways to fight back for centuries. Use the following section to introduce the concept of data liberation and to spark a discussion about resistance.

Tell participants that we are going to substitute the criminalization circle in the venn diagram above with a "Liberation" circle. Use the prompts below to open discussion about this concept.

★ "What comes to mind when you think about liberation?"



Read the definition of data liberation aloud. Take time to define any unfamiliar words or concepts in the definition. Invite further discussion using the prompts below:

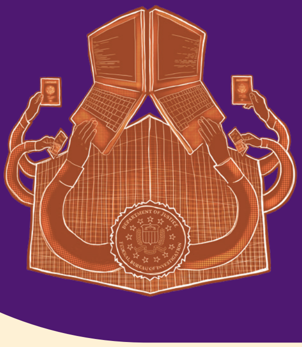
★ "What stands out to you in this definition?"

★ "Can you think of any examples of instances when people and communities have resisted data criminalization?"

Closing 15 min

Give participants an opportunity to reflect on the activity together. You can use any of the following questions to guide the discussion:

- What are some of the major concepts or themes that you learned about during the activity?
- Did any part of the activity surprise you?
- Have you ever thought about data as something that could be created, bought, and sold without your consent? How does that help you think about organizing and targets?
- On the path to data liberation, we need to protect each other…can you think about harm reduction measures that you or your community either has taken or could take to slow down the machinery of data criminalization?



Activity 3:

Challenging Information-Sharing Environments [1]

Workshop Description

This activity offers a deeper exploration into data criminalization, focusing on the systems and actors involved in these processes, and how information sharing is facilitated among them. Begin by providing participants with an overview of the activity:

- We are going to learn some of the key concepts in the report by reading a portion of it together and discussing some of the key takeaways.
- Afterwards, we'll look at an image to identify the systems involved in data criminalization processes.
- We'll conclude the activity by gaining a basic understanding of the concept of interoperability with the goal of identifying potential weaknesses and targets in the data criminalization machinery.

Group Size:
15 -20 People

Workshop Length:
2hr (longer if more people)

Materials:
In person:
Large sheets of paper, markers, copies of illustration

In Person & Virtual:
Access to illustration, Excerpt of *Surveillance Capitalism, Surveillance Carceralism* in the report

Key Terms:
Surveillance
Data Criminalization
Interoperability

Workshop Schedule

10 min	Welcome, icebreaker, community agreements, reviewing goals
40 min	Introduction: Surveillance Capitalism, Surveillance Carceralism
15 min	Break
45 min	Discussion: Understanding Systems and Opportunities for Resistance
10 min	Closing

Introduction: Surveillance Capitalism, Surveillance Carceralism 40 min

Ask participants to form small groups. Groups will read and discuss an excerpt of the *Surveillance Capitalism, Surveillance Carceralism* section in the report. Use the prompts below to invite discussion in the small groups. Once each group has had time to read and discuss, return to the larger group and have groups do share-outs of what they learned.

★ "What themes stand out to you?"

★ "Who are the players/actors involved?"

★ "Can you describe the differences between an event-triggered/watchlist model of criminalization and a big-data model of criminalization?"

[1] The term "information-sharing environment" was borrowed from Ana Muniz's book Borderland Circuity: Immigration Surveillance in the United States and Beyond. She describes one of the primary functions of the TECS platform (a Customs and Border Protection database) as allowing users to access information contained in TECS as well as search over a dozen database systems. This is referred to as interoperability.

Facilitation Tip:

You can adapt this activity by asking volunteers (or pre-selecting them) to take turns reading aloud the chosen reading. Allow extra time for people to read slowly and follow along if you choose this format.

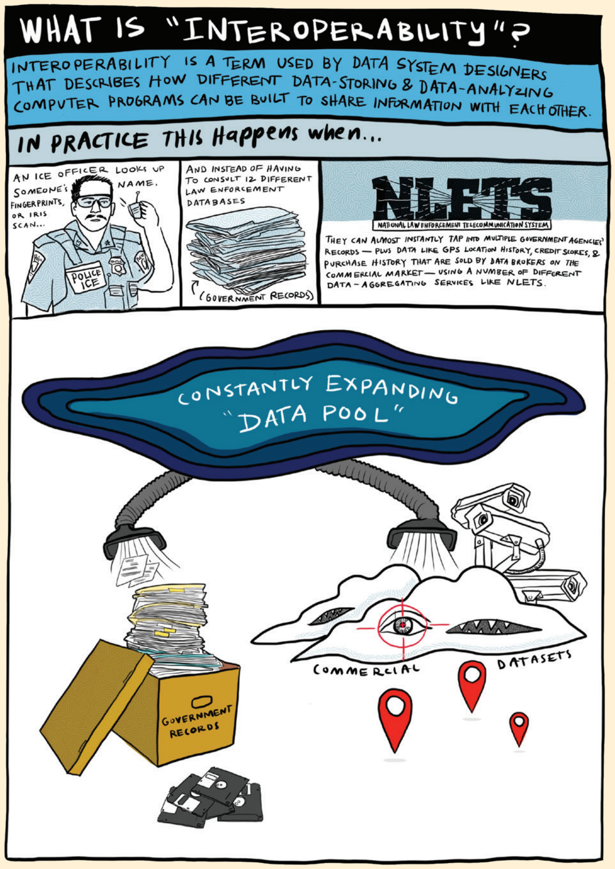
Additionally, we recommend that you outline general themes from the reading beforehand to help you guide the participants in the discussion. Make a list of terms that participants may need support defining throughout the discussion. For example, a basic understanding of the term "immigration detainer" will be needed in subsequent parts of this activity.

Take notes during the share-out on a large sheet of paper (or shared online slide.)

Discussion: Understanding Systems and Opportunities for Resistance 45 min

In this section, participants will be thinking more deeply about the systems involved in data criminalization, including those that facilitate an expansion of the pool of data available to law enforcement for criminalization. Share the illustration with the group and invite everyone to look closely at the image. Invite discussion with the following prompts:

- ★ "What elements do you notice in this image?"
- ★ "Can you offer examples of different actors involved in these processes?"
- ★ "Who or what do you think benefits from these processes of data criminalization?"
- ★ "How do you think interoperability is used for enforcement?"


WHAT IS "INTEROPERABILITY"?
INTEROPERABILITY IS A TERM USED BY DATA SYSTEM DESIGNERS THAT DESCRIBES HOW DIFFERENT DATA-STORING & DATA-ANALYZING COMPUTER PROGRAMS CAN BE BUILT TO SHARE INFORMATION WITH EACH OTHER.
IN PRACTICE THIS Happens when...
AN ICE OFFICER LOOKS UP SOMEONE'S NAME, FINGERPRINTS, OR IRIS SCAN...
POLICE ICE
AND INSTEAD OF HAVING TO CONSULT 12 DIFFERENT LAW ENFORCEMENT DATABASES
(GOVERNMENT RECORDS)
NLETS
NATIONAL LAW ENFORCEMENT TELECOMMUNICATION SYSTEM
THEY CAN ALMOST INSTANTLY TAP INTO MULTIPLE GOVERNMENT AGENCIES' RECORDS — PLUS DATA LIKE GPS LOCATION HISTORY, CREDIT SCORES, & PURCHASE HISTORY THAT ARE SOLD BY DATA BROKERS ON THE COMMERCIAL MARKET — USING A NUMBER OF DIFFERENT DATA-AGGREGATING SERVICES LIKE NLETS.
CONSTANTLY EXPANDING "DATA POOL"
GOVERNMENT RECORDS
COMMERCIAL DATASETS

Discussion: Understanding Systems and Opportunities for Resistance **(Continued)**

Participants were introduced to the concept of interoperability in the previous section. Now, we'll share some examples of systems used by ICE and CBP to foster information-sharing environments. Choose volunteers to assist you in reading the following examples:

NLETS - NLETS is a non-profit telecommunications network that allows 45,000 law enforcement organizations across the country and around the world to share information. It has many functions, but some of the most important ones are as follows: 1) ICE, cops, and other users can log in to the NLETS platform and directly access a plethora of federal and state-level databases to verify information about people. 2) Nlets also enables ICE to send message notifications to state and local law enforcement agencies about people released from their custody into the jurisdiction of that agency.

ICM/TECS - TECS (which is being modernized into ICM) is CBP's international entry/exit log of US border crossings. It is considered a "mammoth" data repository for the copious amounts of data that it collects. Similar to NLETS, users can log in to the TECS platform to both access information contained there, but also simultaneously search over a dozen other public and private law enforcement databases.

Invite discussion about these examples and organizing possibilities using any of the following prompts:

- ★ "What stood out to you in the description of these database systems?"
- ★ "Can you think of examples of how your community may have been impacted by interoperability?"
- ★ "What would you like to learn about how this information is being shared in your local context?"
- ★ "What organizing opportunities do you see considering what we've learned in this activity?"

Closing 15 min

Wrap up the activity by providing a framework for participants that highlights that although government agencies and private companies put huge amounts of money and resources into developing systems of data criminalization, these systems are hugely flawed. This is an opportunity for organizers to find new pipelines to deportation to disrupt.

Give participants an opportunity to reflect on the activity together. You can use any of the following questions to guide the discussion:

- What are some of the major concepts/themes that you learned about during the activity?
- Did any part of the activity surprise you?

Activity 4:
Unmake the Monster

Workshop Description

This activity draws on theater and science fiction to explore what community defense against systems of data criminalization might look and feel like. Participants will learn about DHS databases and then use theater games to think creatively about how to use strategies of community defense against the criminalizing powers of these databases.

No acting experience needed!

Group Size:
5-15 People (Maximum)

Workshop Length:
1 h 30min

Materials:
In person:
Access to Bestiary
OR
Copies of Beast Descriptions and Monster Cards
Large Paper, Markers, Pens, Sticky Notes

Virtual:
Access to online Bestiary, Monster Cards

Key Terms:
Data Criminalization
Community Defense

Workshop Schedule

10 min	Welcome, icebreaker, community agreements, reviewing goals
15 min	Introduction: Meeting the Database Monsters
60 min	Theater Game
	> Overview of the game **(5 min)**
	> Warm-up **(10 min)**
	> Getting to know our database monster **(10 min)**
	> Act it Out! **(10 min)**
	> Getting to know our community defense monsters **(5 min)**
	> Monster Face-Off **(20 min)**
5 min	Closing Circle

Introduction: Meeting the Database Monsters 15 min

In this workshop, participants will be learning about a few key Department of Homeland Security, FBI and commercial database systems. These databases are illustrated on our website in the form of monsters in a "bestiary" (a reference to medieval illustrated books of mythical animals).

NLETS

ICM/TECS

ACRIME

Facilitation Tip:
If the group is able to access the website, invite them to click on the links above to read descriptions of NLETS, ACRIME, and ICM/TECS. Alternately provide paper copies of these descriptions which can be printed from the resource folder.

Invite participants to share responses to these prompts:

- ★ "What stood out to you in the descriptions of each database?"
- ★ "Could any of these databases impact you or your community?"

Theater Game 1 hour

To introduce the theater game, give participants an overview of the activity. Some participants may be nervous about performing/acting. Let everyone know that this game is all about engaging the imagination, no acting experience needed! Although this workshop deals with real and harmful "monsters", ideally the tone of the workshop is welcoming, creative, and fun.

Overview 5 min

- Warm up!
- The group will start by choosing a "monster" (pick the NLETS, ACRIME, or ICM/TECS databases from the last section), and discussing its qualities.
- Everyone will try to act out these qualities together and embody this "database monster" (fun and silliness encouraged!)
- The group will play a game called "UNMAKE the MONSTER". In this game, some participants will continue to act like the   "database monster", while others will be acting as a friendly "community defense monster". The goal of the game will be for the community defense monster to stop the database monster from doing its monstrous activities (e.g. stealing people's data).
- Closing Circle

What is "Theater of the Oppressed"?

This exercise draws on concepts which you may be familiar with through "Theater of the Oppressed" techniques. Feel free to share this background information with participants if desired.

"The Theater of the Oppressed is a participatory theater that fosters democratic and cooperative forms of interaction among participants. It is a 'rehearsal theater' practiced by 'spect-actors' (not spectators) who have the opportunity to both act and observe, engendering processes of dialogue, and critical thinking. In the Theatre of the Oppressed, the theatrical act is experienced as a conscious intervention, as a rehearsal for social action rooted in a collective analysis of shared problems."

Source:
https://hemisphericinstitute.org

Further Resources:
Boal, Augusto. Theatre of the Oppressed. Theatre Communications Group, 1985.
Boal, Augusto. Games for Actors and Non-Actors. Routledge, 2001.

Warm Up 10 min

Guide participants through a warm-up session. Feel free to choose any parts of this which work for your group, or incorporate other warm-up activities of your choice. For an online workshop, invite participants to stretch/move in their own spaces and to embody characters through facial expressions or movements of the upper body.

Guiding Prompts:

- Stand up and/or gently stretch arms up to the sky and down to the ground and then walk/move at a comfortable pace throughout the space ("weaving" through the group) greeting your neighbors as you go.
- Walk/move as slowly as possible and then as quickly as possible through the space (without colliding!)
- Now, it is time to become a monster! Try to move like a swamp monster…. How do you travel through the muddy swamp? Do you lurch forward? Do you slither through the space? Does your body travel low to the ground in a crawl, or do you walk tall with arms reaching out? Experimentation encouraged!
- Return to your normal calm walk, saying "hello" to your neighbors with friendly eye contact as you wrap up the warm-up.

Facilitation Tip:

People may feel silly acting like monsters! The facilitator can help get things rolling by modeling each action for the group (and really going for it!) Remind people that this exercise is not about "getting it right," it is really about being in your body and your creativity.

If moving through the space is not preferable or possible, invite participants to engage in this activity from a seated position.

Getting to Know our Database Monster 10 min

Have the group choose 1 of the 3 database-monsters (from the earlier section "Meeting the Monsters"). Review the monster cards (available in the resources folder) and discuss the qualities with the participants.

Act It Out 10 min

In this section, you will invite the group to embody the database monster. When you read off the first quality, demonstrate the action for the group and invite them to join in (really go for it, encourage playfulness!) Follow the prompts below:

- Read monster qualities one-by-one.
- As you read them, invite participants to embody each quality into their movement, adding more and more qualities to create a dynamic monster character.
    - For example, if "this monster slithers from place to place" AND "loves to eat cell phone data," challenge the group to embody both of these qualities at once! Now try to add even more! (This is a great creative challenge!)
- Once everyone has acted-out several qualities of the monster, regroup.

Getting to Know our Community Defense Monster 5 min

Write “Community Defense Monster” on the top of a large sheet of paper (or shared slide). Invite responses to the prompt below and take notes on participants' responses.

★ “For the purposes of this game, we are going to imagine a friendly monster that will embody qualities of community defense. Now that we have met the database monster we are up against, can we think of what traits we want for our own community defense monster? How would it feel and look to embody those traits?”

Facilitation Tip:

Invite participants to think about what community defense means to them and their organizing context. Feel free to use the definition we’ve provided in the glossary of terms if needed.

Monster Face Off 20 min

Now we are going to have a monster face-off. Ask a small group of people (1-3) to play the role of the Database Monster you have chosen. The rest of the group will be playing the role of the Community Defense Monster. Let the group know that the Monsters will encounter each other and both the Database Monster and the Community Defense Monster will have a chance to say an action they want to take and then act it out.

Ask each group to brainstorm and agree on actions their monster might actually take before beginning the “face-off.” Below some examples:

- A person playing the “NLETS” monster could say… “I am going to share facial recognition data with ICE!” and then act it out by grabbing a prop that represents facial recognition data and handing over that data to ICE.
- People playing the Community Defense Monster could then come up with a response: “We are going to find out how you are collecting that data and figure out how to stop you from doing that!” and then act out looking for the source of the data collection and stopping it in some way.

Once the group grasps the concept, set up the Database Monster and Community Defense Monster to face-off! Get the face-off going by saying “1,2, 3 - Action!” Let people act out data criminalization and defense for whatever time feels appropriate for the energy of the group (lower energy = less time). Pause the scene to give the groups time to confer and pick another round of actions and responses. Or maybe the Community Defense Monster will even strike first with pro-active offense! Let people act out a few rounds as long as the group is engaged. End the scene by having everyone shake it out high-five each other in appreciation for taking risks to be silly and act out monsters.

Facilitation Tip:

Performance in front of a group may feel intimidating. Feel free to check in with participants. Is there anyone who totally loves the spotlight? If only a couple of people want to volunteer to take on these monster roles for the "Face Off" rounds, that can totally work! The rest of the group can participate by sharing what actions each monster should take in this section. Keep the energy snappy and move the group along. End the scene when the energy is high.

Closing Circle 15 min

Ask the group to reflect on:

- What did the Community Defense Monster do to protect and fight back against the Database Monster?
- What community defense do you see in your community or could you imagine being part of?
- What did it feel like to be a Database Monster? A Community Defense Monster? How do we want to feel when we are safe and thriving?

Optional Adaptation: Drawing Game

If you prefer not to lead a theater workshop, but want to try something creative with your group, this workshop can be adapted to focus on imagination through drawing.

Instead of acting out each monster, you can post large sheets of paper on the wall and invite participants to create collaborative drawings. Remind everyone that stick figures are fine! No art experience necessary.

Once you have identified the qualities of the database monster you have chosen to focus on, try to draw them with as much detail as possible, based on those qualities.

Once you have created an image of your database monster, imagine the qualities a community defense monster would need in order to prevent this database monster from continuing to do harm. Invite participants to brainstorm qualities that a community defense monster would need and then add them to a second large drawing. Take time to discuss the qualities the group has added to the community defense monster.

Activity 5:
Reclaiming Sanctuary

Workshop Description

This workshop is intended for organizers who are interested in how data criminalization realities shape organizing. As an example, participants will look at the active collaboration between ICE, DHS, and other law enforcement agencies and how it undermines sanctuary policies. This workshop assumes that participants are familiar with the concepts of "Crimmigration," "P.I.C. Abolition," "Interoperability," "Data Criminalization," and "Data Liberation."

Begin by providing participants with an overview of the activity:

- First we are going to create a mind map with the goal of understanding how patterns of state violence and oppression are connected to data criminalization.
- Then, we will examine sanctuary policies to understand how data criminalization and surveillance have undermined its ultimate goal of providing refuge and safety for people.
- We will wrap up this activity by discussing how these systems relate to local organizing contexts.

Group Size:
15 people

Workshop Length:
2 h 15 min
(longer if more people)

Materials:
In person:
Access to Report & Illustrations
Virtual:
Access to Report & Illustrations

Required Reading:
This workshop requires participants to read approximately 11 pages of the report in advance.

Key Terms:
Crimmigration
PIC Abolition
Data Liberation

Workshop Schedule

10 min	Welcome, icebreaker, community agreements, reviewing the topics
45 min	Introduction: A Mind Map of Data Criminalization
15 min	Break
30 min	Discussion: Constructing Crimmigration, Undermining Sanctuary
20 min	Visioning: Toward Abolitionist Practices
15 min	Closing

Introduction: A Mind Map of Data Criminalization 45 min

Inform participants that we will be creating a mind map using data criminalization as the main concept. Expand outward, making connections between key “actors”, patterns of state violence and oppression, impact of data criminalization, and so on. What connections can we find as a group?

Below some example questions to facilitate the conversation:

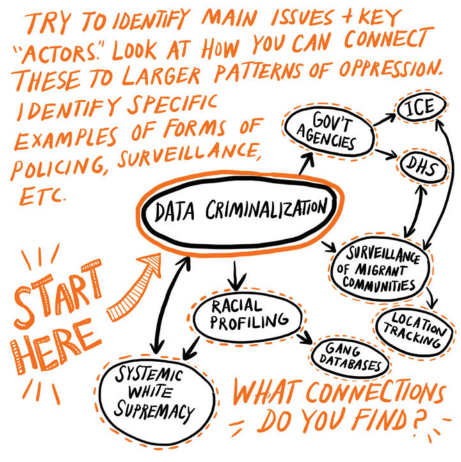
- "What are some real life examples of data criminalization in your city/local context?"
- "How does interoperability figure in these processes?"
- "How are these forms of criminalization used to target immigrants?"
- "Who are some key actors involved in data criminalization?"
- "What are some of the strategies that your communities/ organizations have used to limit or move towards abolition of these forms of criminalization?"

Facilitation Tip:

Decide beforehand what are some of the main categories you want to capture in your mind map, this will help you determine what questions to ask the group in order to populate the map.

For organizers who would like more examples of how to approach creating a mindmap, and who are interested in a deeper dive into ways of visualizing systems of criminalization, refer this resource written and compiled by Micah Herskind:

Mapping the PIC: A Tool for Abolitionist Organizers


TRY TO IDENTIFY MAIN ISSUES + KEY "ACTORS." LOOK AT HOW YOU CAN CONNECT THESE TO LARGER PATTERNS OF OPPRESSION.
IDENTIFY SPECIFIC EXAMPLES OF FORMS OF POLICING, SURVEILLANCE, ETC.
GOV'T AGENCIES
ICE
DHS
DATA CRIMINALIZATION
START HERE
SURVEILLANCE OF MIGRANT COMMUNITIES
RACIAL PROFILING
LOCATION TRACKING
GANG DATABASES
SYSTEMIC WHITE SUPREMACY
WHAT CONNECTIONS DO YOU FIND?

Discussion: Constructing Crimmigration, Undermining Sanctuary 30 min

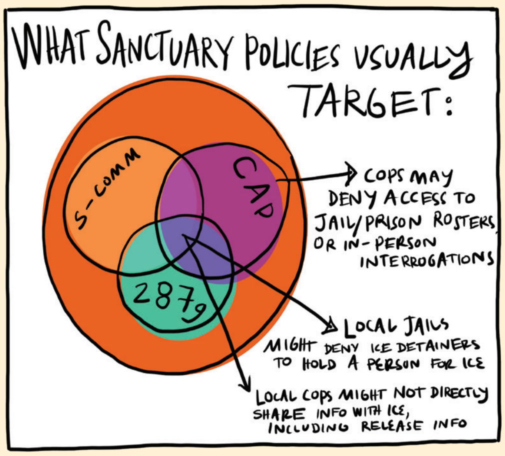
Reviewing the reading: In advance of this workshop, participants will have read a selected portion from the report. Let participants know that we will be discussing the selected reading, and then thinking critically together about some of the infographics from the report.

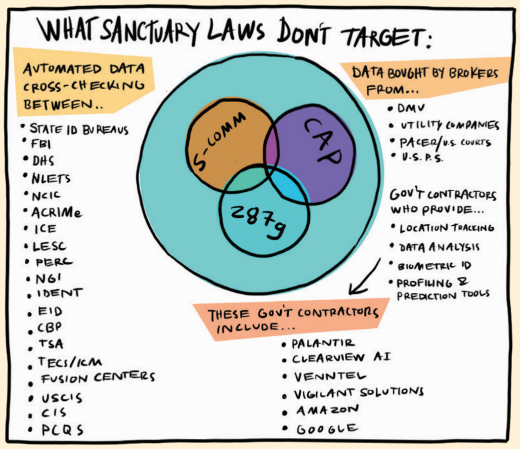
Share with the group the goal of the discussion is not to deny or undermine the importance of organizing for sanctuary policies. The goal is to step back and get a wider view of how state and federal law enforcement collaborate with other entities to undermine these hard-fought protections. Knowing more about how these systems work can offer insight about how to most effectively contest systemic criminalization at a structural level and through an abolitionist framework.

Start the conversation with questions about the reading using the prompts below:

- "What stood out to you about the sections we read?"
- "What are some key takeaways from the reading?"
- "How would you typically define 'sanctuary policy'?"
- "What are some of the ways that data criminalization seems to be undermining sanctuary policies?"

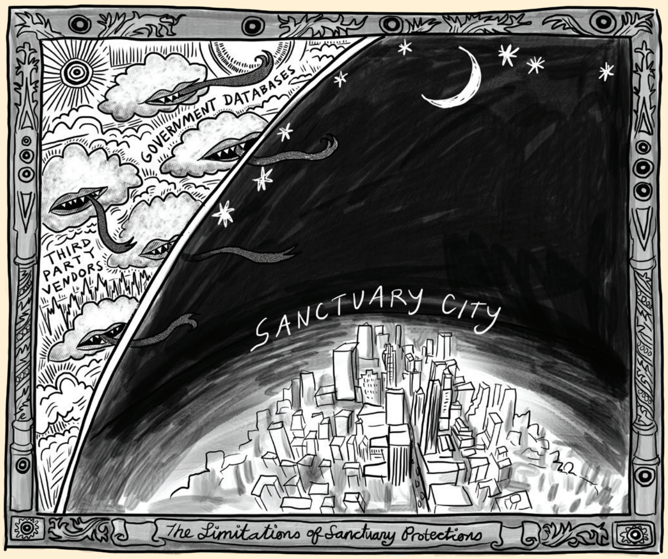
Reviewing Infographics: Now, have participants go into smaller groups to look over the infographics about sanctuary city policies. Make sure you display the images in a large print-out (or slides). Have participants use the discussion questions below for reflections on sanctuary city policies.


WHAT SANCTUARY POLICIES USUALLY TARGET:
S-COMM
CAP
287g
COPS MAY DENY ACCESS TO JAIL/PRISON ROSTERS, OR IN-PERSON INTERROGATIONS
LOCAL JAILS MIGHT DENY ICE DETAINERS TO HOLD A PERSON FOR ICE
LOCAL COPS MIGHT NOT DIRECTLY SHARE INFO WITH ICE, INCLUDING RELEASE INFO



DISCUSSION QUESTIONS:

- What do these graphics show?
- How is it possible for DHS & ICE to access personal data (such as biometric data) even in a Sanctuary City?
- How might they get this information? Who can they collaborate with?
- Is this type of collaboration most local residents know about? What about politicians?



DISCUSSION QUESTIONS:

- What is going on in this image? What do the scary clouds symbolize?
- What are "third party vendors" and how can they undermine sanctuary protections?
- Think back to the reading, what other entities can undermine sanctuary protections?

Towards Abolitionist Practices 20 min

In this section, invite participants to think about abolitionist organizing within the context of data criminalization and how our ongoing learning about data criminalization shapes our campaigns, demands and targets.

Ask for responses to any of these prompts:

- ★ "What work is currently happening in your community that might be impacted or undermined by data criminalization?"
- ★ "What are the limits of laws when it comes to data criminalization?" "How do those limits change how we organize?"
- ★ "What do you want to learn about what data criminalization looks like in your community" "Are there databases, cameras, license plate readers, drones, fusion centers or other criminalizing entities that you want to understand better?" "What do you want to know about them?"
- ★ "What is beyond a sanctuary or a temporary refuge?"

Closing 15 min

Make space for participants to share reflections on the workshop. You can use the questions below to guide the discussion:

- What are some of the major concepts/themes that you learned about during the activity?
- Did any part of the activity surprise you?
- How does this analysis help you think about your local organizing context?

Glossary of Terms

Abolition or **Prison Industrial Complex (PIC) Abolition:**
PIC abolition is a political vision with the goal of eliminating imprisonment, policing, and surveillance and creating lasting alternatives to punishment and imprisonment. Because the PIC is not an isolated system, abolition is a broad strategy. An abolitionist vision means that we must build models today that can represent how we want to live in the future. It means developing practical strategies for taking small steps that move us toward making our dreams real and that lead us all to believe that things really could be different.
Source: Based on a definition by Critical Resistance

Biometrics :
"The measurement and analysis of unique physical or behavioral characteristics (such as fingerprints or voice patterns) especially as a means of verifying personal identity."
Source: Merriam Webster Dictionary

Community Defense :
Work within a community toward the survival and thriving of all members in the face of systemic oppression, harm and violence. The specific strategies toward survival and thriving depend on the specific needs of the community, but often involve forms of mutual aid and collective solidarity.

Constant Vetting:
"Constant vetting" is a term used by entities such as DHS (Department of Homeland Security) and ICE (Immigration and Customs Enforcement) to describe their use of algorithms and prediction tools that continuously surveil the behaviors/activities of U.S. citizens and non-citizens and purport to predict "risk" and potential "criminal" activity.

Crimmigration:
When criminal and Immigration laws intersect, and punish non-citizens in the U.S differently or more harshly than citizens. This double standard is often referred to as "double punishment."

Criminalization:
The action of turning an activity into a criminal offense by making it illegal.

The action of turning someone into a criminal by making their activities illegal.
Source: Oxford Languages

Data:
1. "Facts or information used usually to calculate, analyze, or plan something".
2. "Information that is produced or stored by a computer"
Source: The Britannica Dictionary

Data Criminalization:
The use of data to mark certain people as threats or criminals. Data used to criminalize people is collected from government sources (like fingerprints and arrest records) and commercial sources (like location tracking through smartphone apps). Profiling people based on race, nationality, and religion using data analysis, algorithms, artificial intelligence and biometrics has a long history in the U.S.

Data Liberation:
A data liberation framework rejects the creation and collection of any personal, collective and biometric data by government or private entities for the purpose of criminalization, surveillance or control and is grounded in the values and vision of abolition, self determination
and collective liberation.

Interoperability:
Interoperability is a term used by data system designers that describes how different data-storing and data-analyzing computer programs can be built to share information with each other.

Reformist:
"While 'reform' simply means a change, 'reformist' refers to a kind of liberal political leaning that maintains the current oppressive system by insisting the system is broken and just needs to be fixed. Claiming the PIC (or any of its tools) is broken supports it continuing to exist. Reformist reforms, or reformist change, are about improving institutions so that they can work better. But when an institution is rooted in oppression historically and is designed in order to maintain powerlessness and inequity, making that system work better will increase its ability to inflict harm and violence. If the job of a system is racialized social control, then fixing it to do its job better will improve how it carries out racialized social control. The system needs to be completely uprooted and dismantled in order to end its oppressive power over our lives."
Source: Critical Resistance's Abolish Policing Toolkit

Surveillance:
The non-consensual observation of individuals and communities by state, corporate or academic entities who have power to make meaning from, exert control over, exploit or otherwise profit from an observed population. Surveillance is active intervention in the form of behavior prediction for modification; it is real-time social control.

Surveillance Capitalism:
Ways in which our daily lives, experiences, and interactions are mined for data for the purposes of behavior prediction and control under capitalism. Data is mined via our interactions with consumer goods (such as biometric data capture from smartphone apps, etc.) which can be aggregated with other data points and sold..

Surveillance Carceralism:
Systems of confinement, control, prediction, punishment and regulation which can include but also extend beyond the physical enclosures of prisons. These systems use digital prediction and analytic tools that direct policing, abandonment, social control and state violence. In contrast with "surveillance capitalism," the term "surveillance carceralism" highlights the ways that digital tracking and prediction target criminalized populations differently than people given legal rights.

Third Party Vendors:
Any company, individual or organization that has been contracted to provide a service on behalf of another entity is a third-party vendor.
Government entities such as DHS (Department of Homeland Security) frequently contract with or buy data from companies who collect data from commercial services. It is financially profitable for these companies to collect and analyze data from commercial sources in order to create predictive models for where potential customers may travel, what kinds of products they may want to buy, etc.

When a government entity like DHS works with these companies, DHS gains access to personal data which was "willingly" (but often unknowingly) given to a commercial service such as a smartphone app by a consumer. Access to this data gives DHS a legal and warrant-free way to acquire information such as GPS location data, biometric data, etc., which can be used for purposes of data criminalization.

White Supremacy:
"White Supremacy describes a system of power that has its historical roots in the European effort for social, political, economic, and geographical dominance. This system of power is also key to how the U.S. has been organized to systematically benefit white people and act out of violence on people of color"
Source: Based on a definition by Critical Resistance

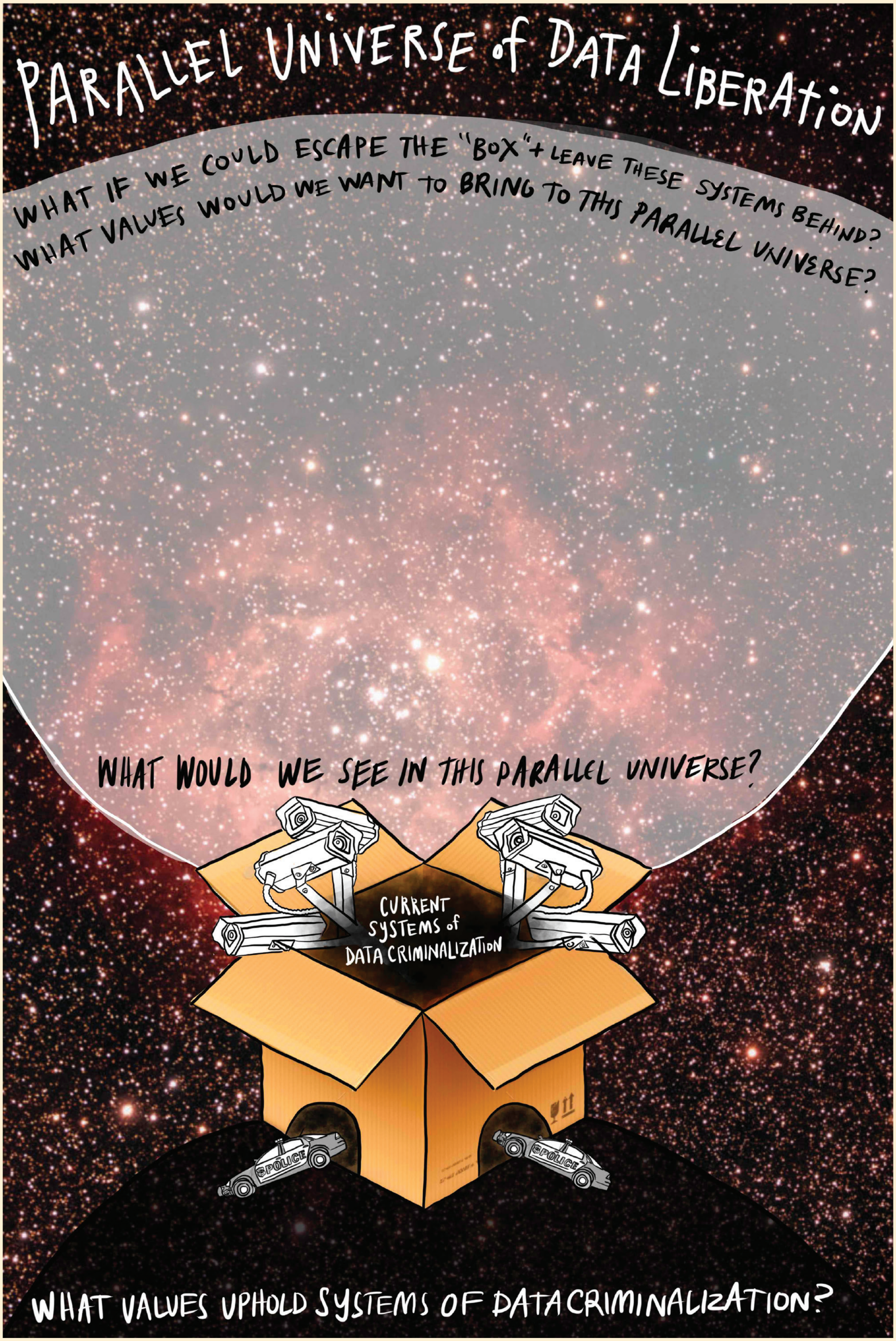
ABOLISH DATA CRIMINALIZATION

WORKBOOK RESOURCES

Activity 1:

The Monster Quiz

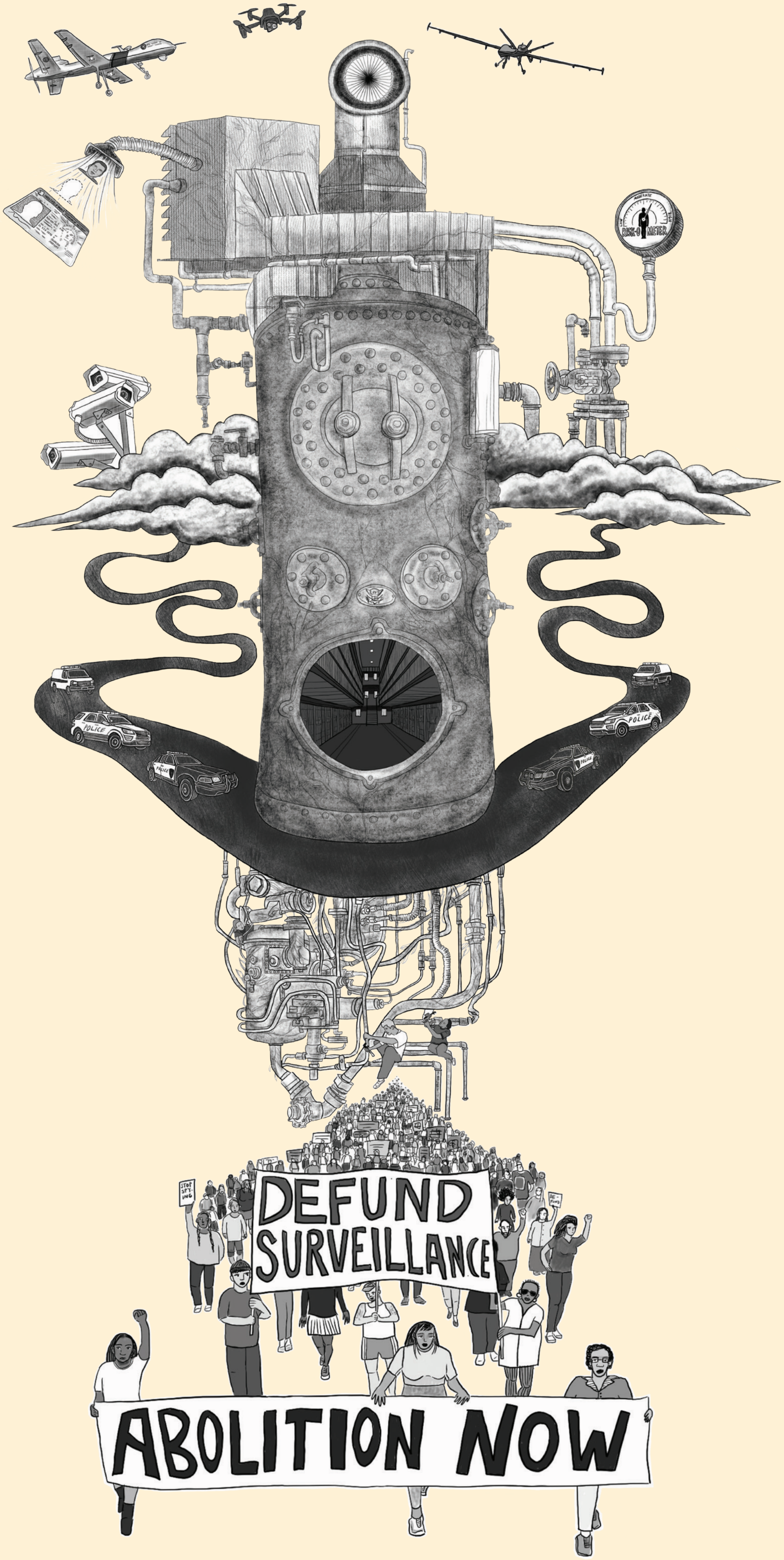
ACCOMPANYING RESOURCES: Illustration


PARALLEL UNIVERSE of DATA LIBERATION
WHAT IF WE COULD ESCAPE THE "BOX" + LEAVE THESE SYSTEMS BEHIND?
WHAT VALUES WOULD WE WANT TO BRING TO THIS PARALLEL UNIVERSE?
WHAT WOULD WE SEE IN THIS PARALLEL UNIVERSE?
CURRENT SYSTEMS of DATA CRIMINALIZATION
POLICE
POLICE
WHAT VALUES UPHOLD SYSTEMS OF DATA CRIMINALIZATION?

* Examples of real-life data criminalization:

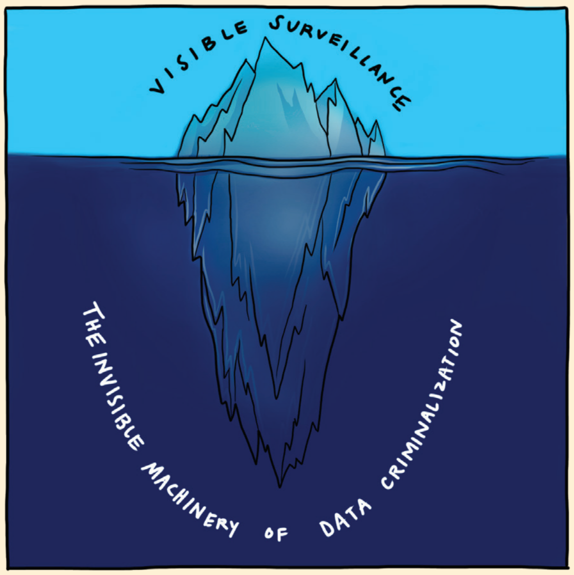
- You receive a Facebook message from a stranger whose account has a profile photo of a dog. The writer says that they want to meetup and buy a piñata that you're selling. An ICE officer greets you in the parking lot.[1]
- The salesperson at the car lot refuses to sell you a car after running a credit check and finding that TransUnion, a credit reportingagency, flagged your name as a "potential match" for one on the Treasury Department's watch list for "terrorists, drug traffickers and other criminals." [2]
- The highway patrol officer who just ran your license decides to detain you, based on the automated alert that he received that alleges that you were previously deported.[3]
- ICE agents arrive at the airport gate before you catch an international flight.[4] A computer system identified you as a risk for having overstayed a visa.[5]
- ICE shows up at your non-immigration-related court appointment.[6]
- A detainer and an administrative warrant are served to a jail, asking the Sheriff to notify ICE when you'll be released.[7]
- You receive an order of removal.[8]

*This is an excerpt of the report *From Data Criminalization to Prison Abolition*. Full text available **here**.


MODERATE
LOW
HIGH
RISK-O-METER
POLICE
POLICE
POLICE
POLICE
STOP SPY-ING
DE-FUND
DEFUND SURVEILLANCE
ABOLITION NOW

Activity 3:
Challenging Information-Sharing Environments
ACCOMPANYING RESOURCES: Selected Reading and Illustration

* SURVEILLANCE CAPITALISM, SURVEILLANCE CARCERALISM



GENERALLY, THE SURVEILLANCE THAT WE CAN SEE MAKE UP THE TIP OF AN ICEBERG:

- You receive a Facebook message from a stranger whose account has a profile photo of a dog. The writer says that they want to meetup and buy a piñata that you're selling. An ICE officer greets you in the parking lot.[1]
- The salesperson at the car lot refuses to sell you a car after running a credit check and finding that TransUnion, a credit reportingagency, fl agged your name as a "potential match" for one on the Treasury Department's watch list for "terrorists, drug traffickers and other criminals." [2]
- The highway patrol officer who just ran your license decides to detain you, based on the automated alert that he received that alleges that you were previously deported.[3]
- ICE agents arrive at the airport gate before you catch an international flight.[4] A computer system identified you as a risk for having overstayed a visa.[5]
- ICE shows up at your non-immigration-related court appointment.[6]
- A detainer and an administrative warrant are served to a jail, asking the Sheriff to notify ICE when you'll be released.[7]
- You receive an order of removal.[8]

For every one of those encounters there is much unseen: troves of data sorted and choices made by algorithms, dozens of analysts and agents, billions of dollars in contract vendors, a daisy-chain of computers and communications systems and interoperable software programs, mirrored datasets and cloud servers, a miasma of agencies and interfaces.

Today's sprawling surveillance machinery of immigrant criminalization was built over decades, drawing from centuries of racialized capitalism and social control, anti-blackness, settler-colonial expansionism, and US imperialism.

*This is an excerpt of the report *From Data Criminalization to Prison Abolition*. Full text available **here**.

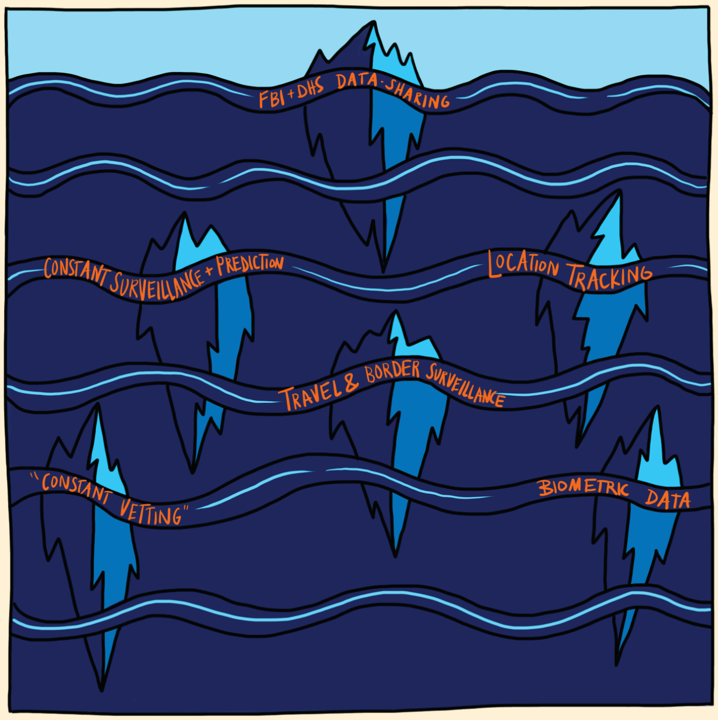
Through evolving surveillance practices of data criminalization, the US government creates and uses data as both justification for and a means to criminalize US non-citizens. The term "crimmigration" refers to the intersection of criminal and immigration laws in the US, especially since the 1990s, to punish non-citizens in the US differently and more harshly.[9] Crimmigration developed alongside and as part of mass incarceration. The artifacts and outcomes of that "crimmigration" history is preserved in numerous people's "permanent records" in legacy and cutting-edge government databases, and in data-sharing protocols built into law enforcement technology and communication tools.[10]

These databases are not just an archive; they are an arsenal.

These databases are not just an archive; they are an arsenal. New prediction and profiling technologies contracted by DHS grow the agency's migrant surveillance dragnet by dredging up decades-old, often forgotten data (including data not originally intended to criminalize, such as naturalization and passport application records) and gives that data new life to criminalize by matching them with previously unlinked criminal records and newer forms of invasive biometric identification and location-tracking databanks. But a "match" to criminal records, flagged by an event such as international travel, or getting stopped by a cop, is no longer the only path to immigrant criminalization.

...a "match" to criminal records, flagged by an event such as international travel, or getting stopped by a cop, is no longer the only path to immigrant criminalization.

In DHS' newer data-sorting mechanisms, artificial intelligence (AI) tools are capable of scanning millions of database entries, collecting new data, creating "profiles" of individuals, linking them to others, and using so-called predictive analysis to sort people categorically for ICE to monitor and revisit based on assigned levels of "risk."[11] And, for as many dollars as have been invested into databases, analysts, and prediction, there are even more errors and omissions. Records are flush with name misspellings, outdated naturalization records and incomplete adjudication records. ICE has stated that there are a few million people who "derived' citizenship (people who were not born in the US but became citizens at birth, or at some point while still a minor, because of their parents' status), whom DHS databases would flag as non-citizens based only on their birth abroad.[12] Police are able to include in gang databases anyone that they want. Gang databases list deceased people and infants as members.[13] Data analyses are often incorrect, relying on outdated or inaccurate data, and they have outsized impact. Each past "encounter" that a person has had with a customs agent, immigration officer, or cop creates lasting vulnerability and exposure that can be reactivated if a person falls into a category (for instance, naturalized citizens, current visa holders, non-citizens, or people who are "removable" by ICE) that are flagged for increased scrutiny by DHS. Categorically targeted people are added to various databases who will be automatically and constantly tracked, profiled and evaluated for deportability — as well as disciplined by being denied public benefits, workplace protections and other access to rights.



WE ARE AT A CROSSROADS

In the following sections, we examine how key law enforcement databases have been connected and updated for decades, noting potential targets in these automated, linked systems. We describe the significance of DHS' move from a suspect-based "watchlist" model to a big data model, monitoring massive numbers of individuals in real time and circumventing legal and all other oversight by buying GPS and cell phone location data, utility bills, DMV records, Internet search history,[14] change-of-address records, social media interactions, and other personal information that is routinely sold to government agencies by commercial vendors. We name some common points of data extraction, old and new. We also provide an overview of traveler and US border surveillance since the late 1990s, because monitoring techniques for international travel have been at the forefront of data criminalization and surveillance and may foretell the next decade of immigration and criminal punishment enforcement technologies.

DHS's digital surveillance system is still in its infancy, and thus seemingly inefficient.[15] Despite the vast amount of resources that DHS receives, since its inception the agency has been plagued by rivalries, bureaucracy, high turnover and lack of consistent leadership due to changes in US presidential administrations.[16] One former management-level DHS employee noted that at the time of its creation, "DHS wasn't even a loose confederation of agencies, back then it was more like rogue nations that happen to find themselves on the same continent."[17] Conflicts between sub-agencies ("DHS Components") have prevented seamless database merging.[18] And logistical problems persist. ICE needs to physically locate a person in order to arrest and potentially deport them. Deportation can be a time-intensive process. ICE officers have large caseloads and need to work with embassies and consulates to obtain travel identification documents, such as birth certificates and passports, which permit ICE to deport a person.[19] Despite the billions of dollars ICE spends on sophisticated spying, data visualization, indexing and prediction tools, the process of deporting people from inside of the US can still require accessing standardized criminalization data and engaging in a bureaucratic legal process.

Court records show that one of DHS' major criminalization hubs, the Pacific Enforcement Response Center (PERC) — which hires analysts to work 24/7 and use top-of-the-line data-scraping and social-mapping tools to find people who might be deportable — issued nearly 50,000 detainers in FY 2019. [20] Yet, "trial evidence nevertheless indicated that ICE does not take into custody up to 80 percent of the individuals for whom PERC issues immigration detainers." Recent data collected by Syracuse University's Transactional Records Access Clearinghouse (TRAC) confirm the pattern.[21]

WHAT IS "INTEROPERABILITY"?

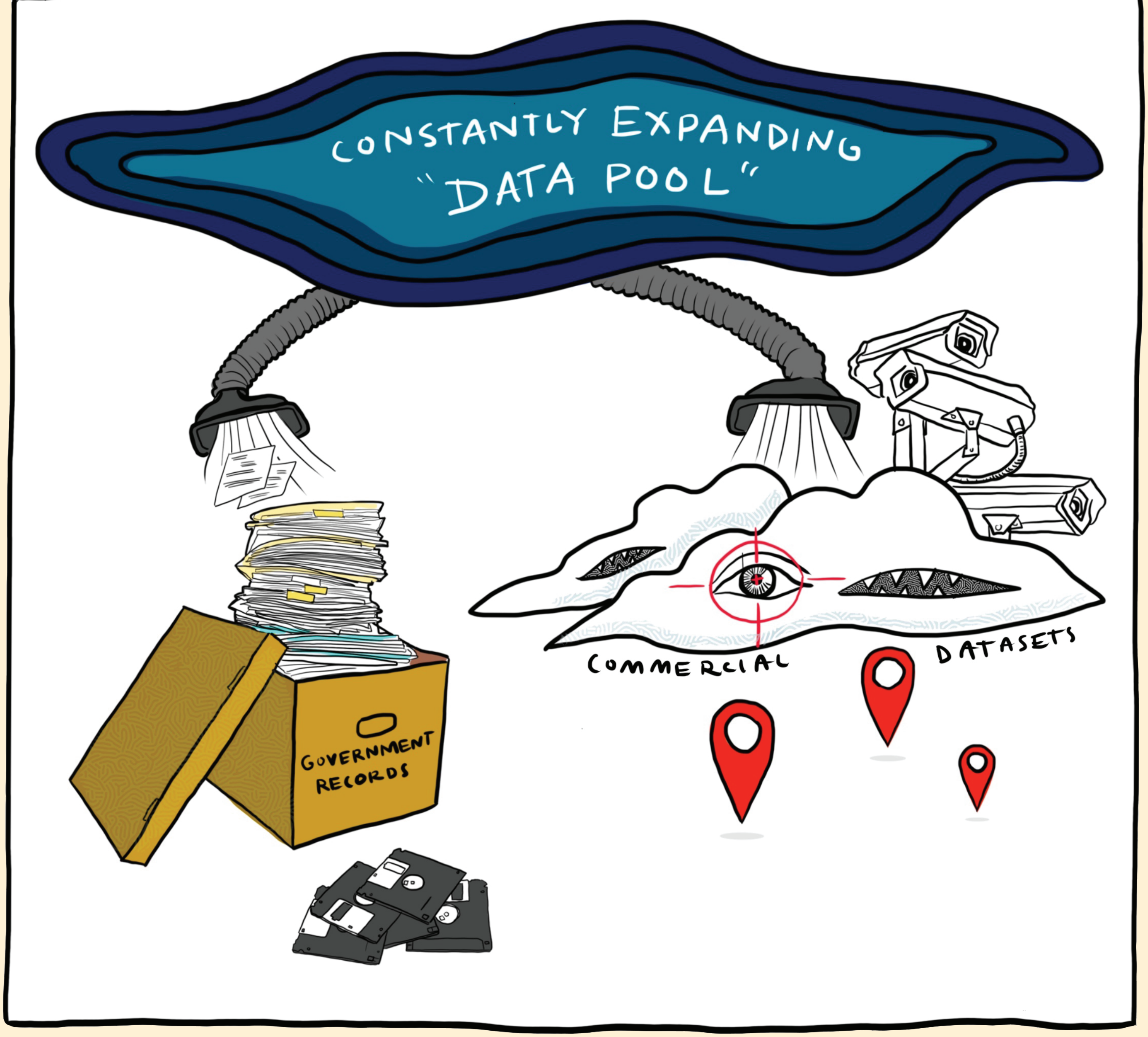
INTEROPERABILITY IS A TERM USED BY DATA SYSTEM DESIGNERS THAT DESCRIBES HOW DIFFERENT DATA-STORING & DATA-ANALYZING COMPUTER PROGRAMS CAN BE BUILT TO SHARE INFORMATION WITH EACH OTHER.

IN PRACTICE THIS Happens when...

AN ICE OFFICER LOOKS UP SOMEONE'S NAME, FINGERPRINTS, OR IRIS SCAN...

AND INSTEAD OF HAVING TO CONSULT 12 DIFFERENT LAW ENFORCEMENT DATABASES

THEY CAN ALMOST INSTANTLY TAP INTO MULTIPLE GOVERNMENT AGENCIES' RECORDS — PLUS DATA LIKE GPS LOCATION HISTORY, CREDIT SCORES, & PURCHASE HISTORY THAT ARE SOLD BY DATA BROKERS ON THE COMMERCIAL MARKET — USING A NUMBER OF DIFFERENT DATA-AGGREGATING SERVICES LIKE NLETS.



Activity 4:

Unmake the Monster

ACCOMPANYING RESOURCES: Monster Information & Cards

ICM/TECS

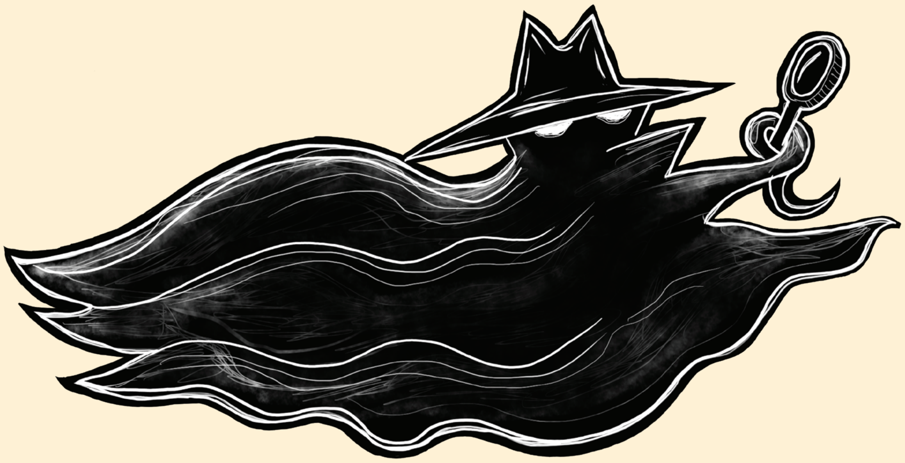
TECS, CBP's international entry/ exit log of crossings of US borders since 1987, is being "modernized" into ICM, an "intelligence system" and database index built by the Silicon Valley tech company, Palantir. ICM is based on Palantir's off-the-shelf Gotham tool designed for police departments, but is configured specifically for DHS' Homeland Security Investigations.

ICM allows instantaneous search of other government intelligence platforms such as the Drug Enforcement Administration, Bureau of Alcohol, Tobacco, Firearms and Explosives, and the FBI. ICM can access AFI (also made by Palantir, and detailed below) and can query ACRIMe. Users of ICM can access both government-owned and private criminalizing databases and biometric data.[1] These include the FBI Terrorist Screening Center's Terrorist Screening Database,[2] NCIC,[3] and Nlets.[4]

Since 1987, CBP officers have used TECS as their main system at the border and elsewhere to screen arriving travelers and determine their admissibility. TECS recorded law enforcement "lookouts," border screening data, and reporting from CBP's primary and secondary inspection processes. TECS includes free-form notes written by CBP officers and Border Patrol agents about individuals with whom they interact. CBP officers and Border Patrol agents can allege that someone's behavior might be related to intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention; this notation will stay on a person's permanent record, regardless of the outcome of the encounter.[5]

Buying an airline ticket for an international flight creates a flag in the TECS system if you are already being tracked in the database.[6] ICE analysts can sign up for notification alerts, so if you have a final order of removal, for example, and purchase an international airline ticket in your name, ICE can send agents to meet you at the airport.[7]

*These are three of the twenty-one databases that comprise our DHS Database Bestiary. All of the other databases can be found **here**.



NLETS

Nlets is a telecommunications network that is a backbone of today's migrant data criminalization machinery, sharing information between 45,000 law enforcement organizations nationally and internationally, and checking the fingerprints of anyone booked by police against DHS records.

Nlets allows police, ICE and other users of its system to directly access the state-level databases that feed into the NCIC in order to verify the information obtained through NCIC searches.[1] Nlets allows users to query federal law enforcement and multiple states at once if they have a person's name and other biographical details.[2] Depending on varying state rules, Nlets might provide a person's Social Security Number and home address, and parole, probation, and criminal legal history information that goes beyond what can be found in NCIC and other federal and state information-sharing pipelines. Additionally, Nlets includesand shares driver's license information, including photos[3] for facial recognition,[4] and motor vehicle registration information.

Nlets is a key system used in the automated, computerized fingerprint checking process that cross-checks everyone booked by non-immigration police against DHS datasets. If ICE has to release a person from custody, and that person was ever convicted of a violent or serious crime (defined by ICE as homicide, sexual assault, aggravated assault, or robbery), ICE uses Nlets to send message notifications to state and local law enforcement agencies in the jurisdiction where a person is released or where they intend to reside. The notification informs local law enforcement when and where that person will be released.[5]

Nlets is multiple things, and worth examining as a target: It is a more than fifty-year-old "private not-for-profit partnership" of fifty states, law enforcement agencies and corporate partners.[6] It has been operational at least since the late 1990s, and is a cloud-based network that includes criminal records and personal data.[7] According to a 2014 Justice Research and Statics Association article, "Nlets is governed by its representatives. Principle member agencies, (e.g., state police departments, departments of public safety, and bureaus of investigation) each appoint a representative. Collectively, these representatives elect officers and a Board of Directors. Along with their governing responsibilities, representatives serve as the primary Nlets contact for their agencies' interstate data exchange."[8] Yet, law professor Bridget A. Fahey wrote, Nlets "acts like a private entity, not a government institution, though it serves as gatekeeper to a sweeping amount of government data."[9] For instance, Nlets shares information with its partner private companies, which in turn develop surveillance technologies for law enforcement.

According to its 2020 ICE Office of Acquisition Management budget justification document, ICE stated, "Based on Market Research, no other vendor can provide the same unique services that Nlets provides to the LESC."[10] As Just Futures Law noted in its 2020 report on Nlets, "It is important to understand that state participation in Nlets, along with many other national or regional data exchanges, is voluntary. States can choose not to share information or limit the type of informatio shared through Nlets. Some states have already chosen not to share certain information, such as driver's license photos, through Nlets."[11]

ACRIME

ALIEN CRIMINAL RESPONSE INFORMATION MANAGEMENT SYSTEM

Three ominous beings with surveillance cameras in place of heads appear to rise from a dark cloud. Office buildings reminiscent of F.B.I. headquarters rest on the cloud. Three mouths full of sharp teeth hover within the cloud.

Alien Criminal Response Information Management System (ACRIMe) is a web-based ICE data system used by contract analysts at ICE's Law Enforcement Support Center (LESC) to access criminal legal and DHS databases in order to cross-reference a person whose immigration status is unknown. ACRIMe allows ICE's contract analysts and field officers to access some criminal legal and DHS sub-agency files, respond to immigration status queries, or tag targeted individuals in FBI and criminal law enforcement files for future "lookout."[1] ACRIMe automatically searches for name and date of birth matches in various criminal, customs, and immigration databases.[2] In addition to government datasets, a person using ACRIMe can also choose to manually search other government and commercial databases.[3] Data fed into commercial data aggregators come from numerous government and other commercial databases.[4] These include real-time incarceration records (including booking photos), cell phone location and automated license plate reader data history, utility information from Equifax, and social media accounts.

ACRIMe allows ICE field officers to access the analyst's research. Based on those searches, ICE's data analyst decides whether ICE has the basis to issue a detainer or arrest you.

ACRIMe is used to prepare an Immigration Alien Response (IAR) that recommends to an ICE deportation officer whether you might be removable.[5]
The IAR includes a person's last known immigration or citizenship status, basic biographical inform tion and criminal history. ACRIMe then electronically returns the IAR to both the requesting agency and the ICE ERO Field Office that is in the region of the requestor. If the analyst decides that a person might be deportable, then an ICE agent or officer can lodge a detainer via the ACRIMe system, and the IAR is routed to the local ICE field office which has jurisdiction.[6]

ICM/TECS

Description:
TECS, CBP's international entry/ exit log of crossings of US borders since 1987, is being "modernized" into ICM, an "intelligence system" and database index built by the Silicon Valley tech company, Palantir. ICM is based on Palantir's off-the-shelf Gotham tool designed for police departments, but is configured specifically for DHS' Homeland Security Investigations.
Monster's "vibe"= Wild West cyber cowboy-cop

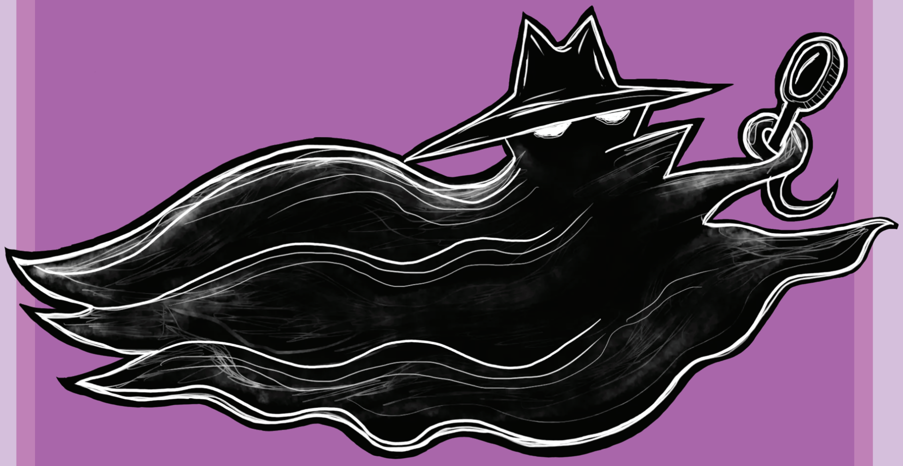
Monster's Location:
The US-Mexico border, and Palantir HQ

Mode of Travel:
ICM/TECS is a cyborg with robotic legs. This monster gallops like a horse along the U.S. Border.

Favorite Food:
ICM/TECS loves to eat "border admissions" records.

Monster's Relationships:
Close homies with Palantir fam and CBP databases. Really tight with AFI and ACRIMe. Gets stronger every time a Border Patrol agent stops and harasses someone.

Monster's Belief System/Ideology:
"Technological utopianism"- As an updated and highly interconnected database (connected to Drug Enforcement Administration, Bureau of Alchohol, Tobacco, Firearms, and Explosive, and FBI) which has consolidated entry-exit records (border admissions) into a searchable database which include "prior criminal history" ICM TECS is bringing xenophobic "Wild West" vibes to a whole new hi-tech level...



NLETS

Description:
Nlets is a telecommunications network that is a backbone of today's migrant data criminalization machinery, sharing information between 45,000 law enforcement organizations nationally and internationally, and checking the fingerprints of anyone booked by police against DHS records.

Monster's Location:
This monster travels in the "cloud", but originated in paper records and card catalog systems in U.S. jails.

Mode of Travel:
NLETS hovers in the air and drifts from one government agency to the next.

Favorite Food:
Old Government Records.

Monster's Relationships:
Best Friends = Cops (because they only get to use their monster powers when cops arrest someone), "Frenemies" with ACrime (a newer database that is replacing them).

Monster's Belief System/Ideology:
"Take a Bite Out of Crime!" Believes in "old school" (Reagan-era) tough-on-crime approach.

ACRIME

Description:
Alien Criminal Response Information Management System (ACRIMe) is a web-based ICE data system used by contract analysts at ICE's Law Enforcement Support Center (LESC) to access criminal legal and DHS databases in order to cross-reference a person whose immigration status is unknown.

Monster's Location:
This monster is a database that connects the physical locations of LESC, PERC, ICE Field offices and individual ICE agents carrying mobile devices that access "ACRIMe Field" with the Internet and commercial databases.

Mode of Travel:
ACRIME floats along pathways of wireless communication, summoned from place to place by ICE agents.

Favorite Food:
Biometric data found in commercial databases. ACRIME loves cloud-based data and eats it like cotton candy!

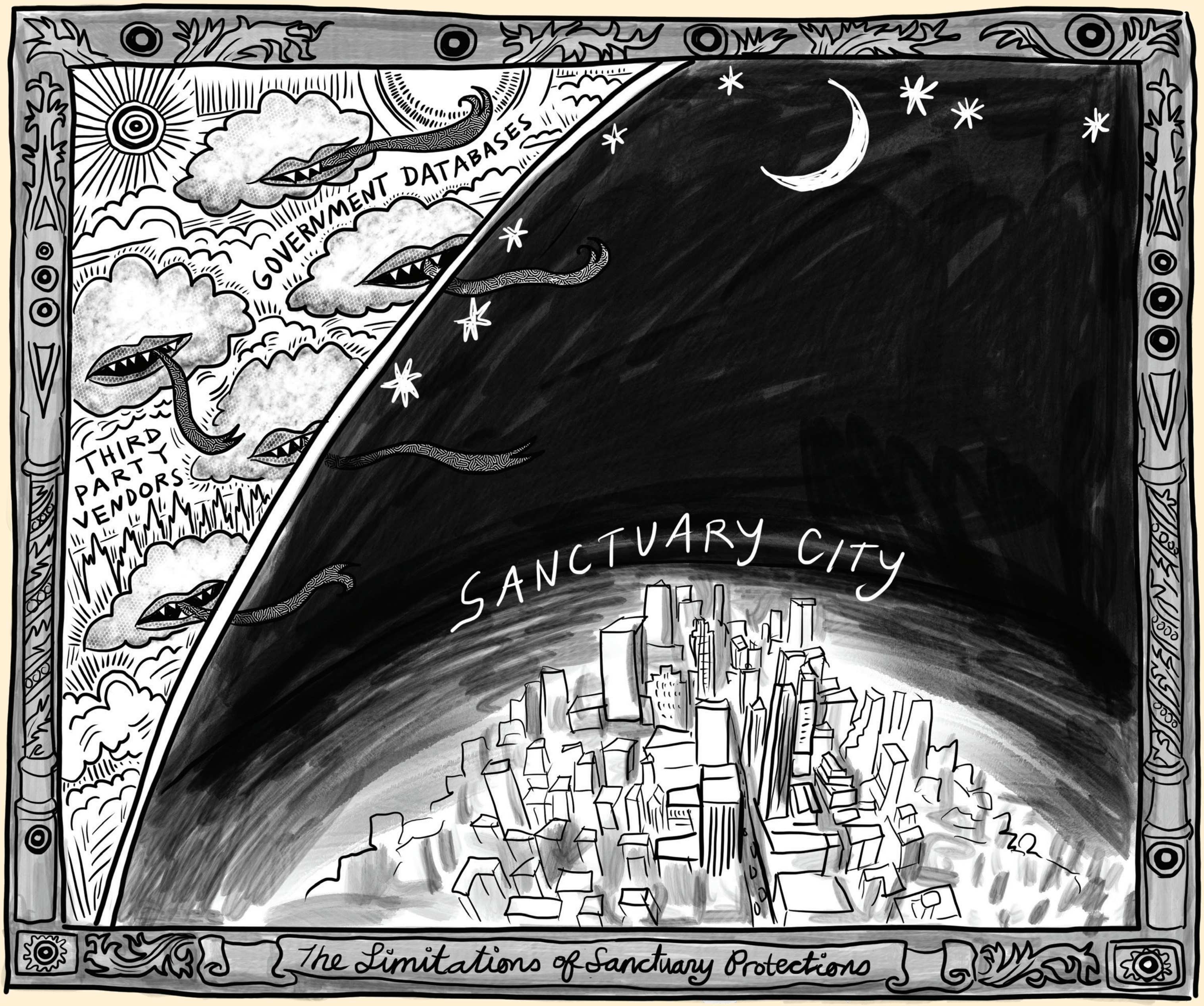
Monster's Relationships:
Semi-playful rivalry with Nlets... taking some of their work away from them as a messenger/ delivery system between law enforcement agencies w/ ICE, and between ICE, LESC and PERC.

Monster's Belief System/Ideology:
Very detail-oriented bureaucratic monster. Fixted on the process of criminalization, if they believe in anything it is "order" with no regard to people's lives.

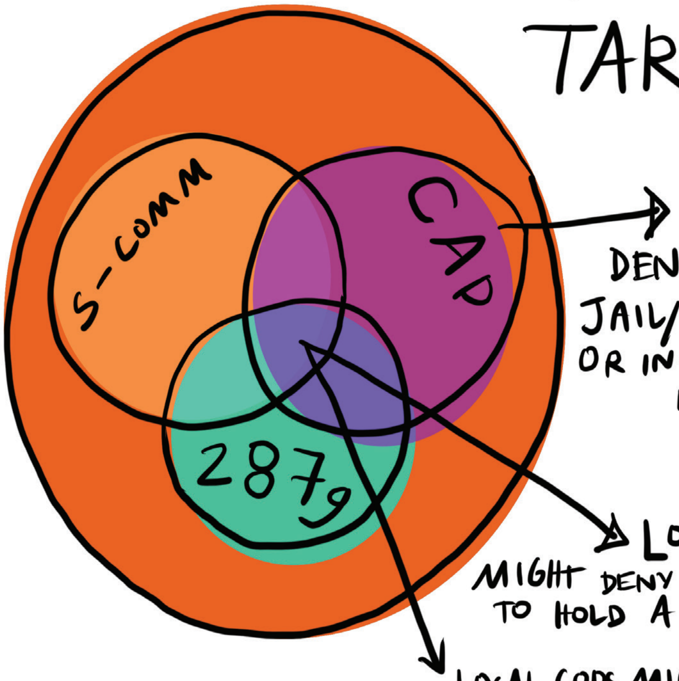
Activity 5:

Reclaiming Sanctuary

ACCOMPANYING RESOURCES: Illustrations & Selected Reading



WHAT SANCTUARY POLICIES USUALLY TARGET:



COPS MAY DENY ACCESS TO JAIL/PRISON ROSTERS, OR IN-PERSON INTERROGATIONS

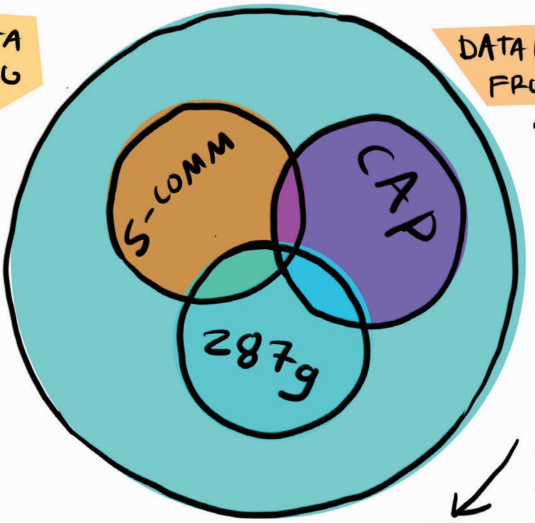
LOCAL JAILS MIGHT DENY ICE DETAINERS TO HOLD A PERSON FOR ICE

LOCAL COPS MIGHT NOT DIRECTLY SHARE INFO WITH ICE, INCLUDING RELEASE INFO

WHAT SANCTUARY LAWS DON'T TARGET:

AUTOMATED DATA CROSS-CHECKING BETWEEN..

- STATE ID BUREAUS
- FBI
- DHS
- NLETS
- NCIC
- ACRIMe
- ICE
- LESC
- PERC
- NGI
- IDENT
- EID
- CBP
- TSA
- TECS/ICM
- FUSION CENTERS
- USCIS
- CIS
- PCQS



DATA BOUGHT BY BROKERS FROM...

- DMV
- UTILITY COMPANIES
- PACER/U.S. COURTS
- U.S.P.S.

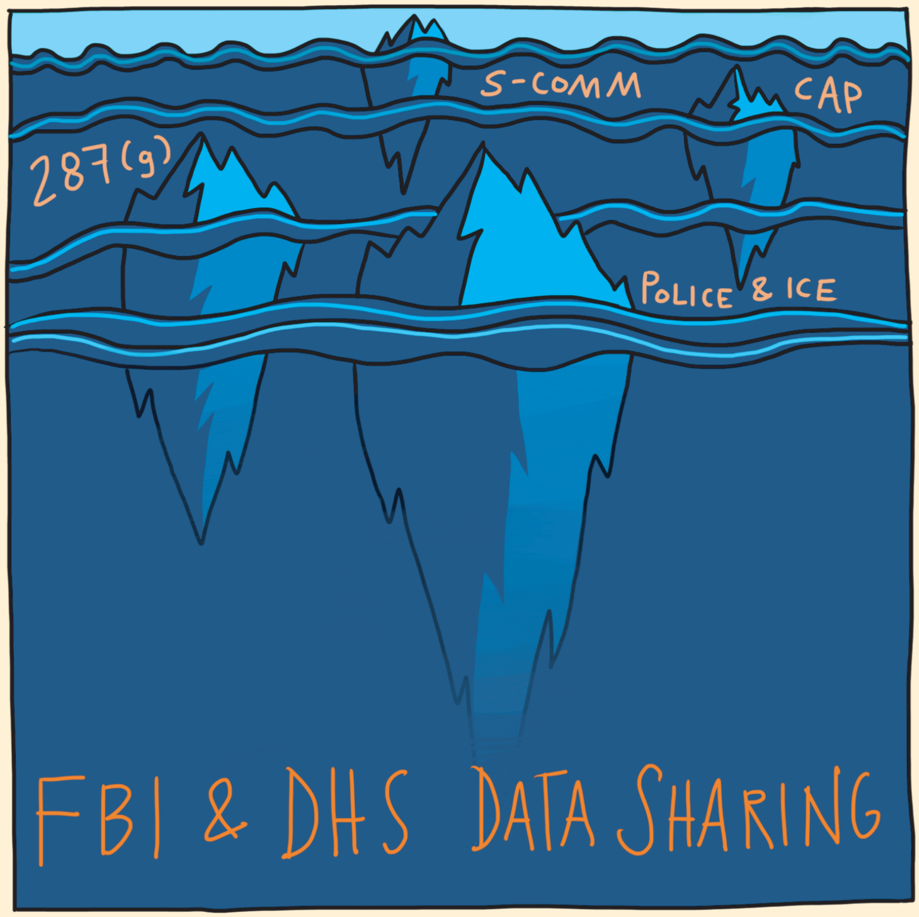
GOV'T CONTRACTORS WHO PROVIDE...

- LOCATION TRACKING
- DATA ANALYSIS
- BIOMETRIC ID
- PROFILING & PREDICTION TOOLS

THESE GOV'T CONTRACTORS INCLUDE...

- PALANTIR
- CLEARVIEW AI
- VENNTEL
- VIGILANT SOLUTIONS
- AMAZON
- GOOGLE

* FEEDBACK LOOPS OF ENDLESS CRIMINALIZATION



In the following sections, we examine how data criminalization operates within:

1. Police encounters and profiling
2. Automated data-sharing systems used by law enforcement agencies
3. Surveillance capitalism: the expanding market of data brokers, cell phone apps, social media and digital stalking
4. Biometric technologies and covert identification practices
5. Traveler surveillance and securitization
6. Bureaucratic pathways to visas and naturalization

For this report, we do not aim to provide a complete taxonomy of all government and commercial databases used to criminalize, but instead ask how the tangled and blurry morass that we can discern might indicate how a larger machinery operates.

*This is an excerpt of the report *From Data Criminalization to Prison Abolition*. Full text available **here**.

CONSTRUCTING CRIMMIGRATION

Collaborations and data-sharing between law enforcement and ICE have been the most efficient way to criminalize and deport record numbers of immigrants from the US. The majority of ICE arrests are based on hand-offs from jails and prisons directly to ICE. A 2020 DHS Office of the General Inspector audit analyzed Enforcement and Removal Operations (ERO) data from 2013-2019 and found that "516,900, or 79 percent of its 651,000 total arrests, were based on in-custody transfers from the criminal-justice system."[1]

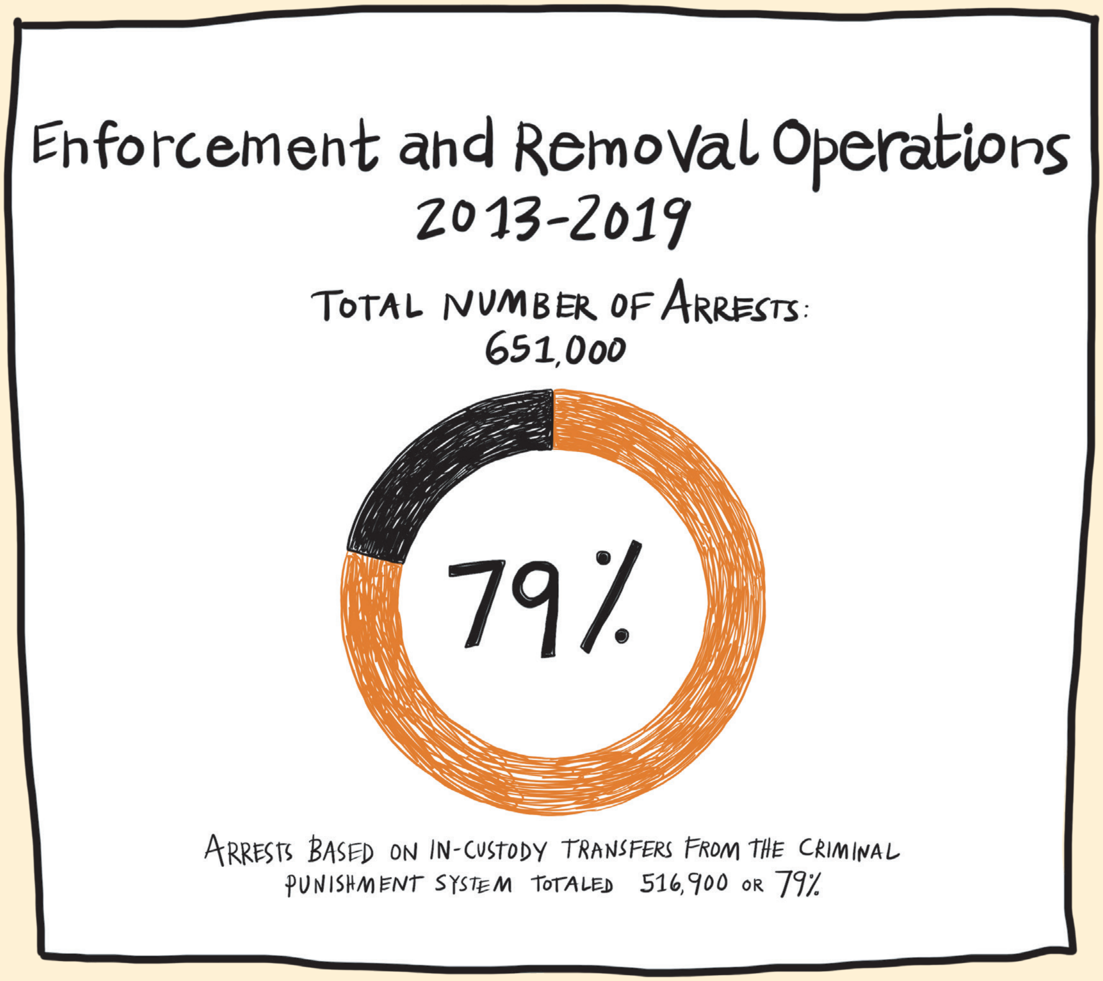


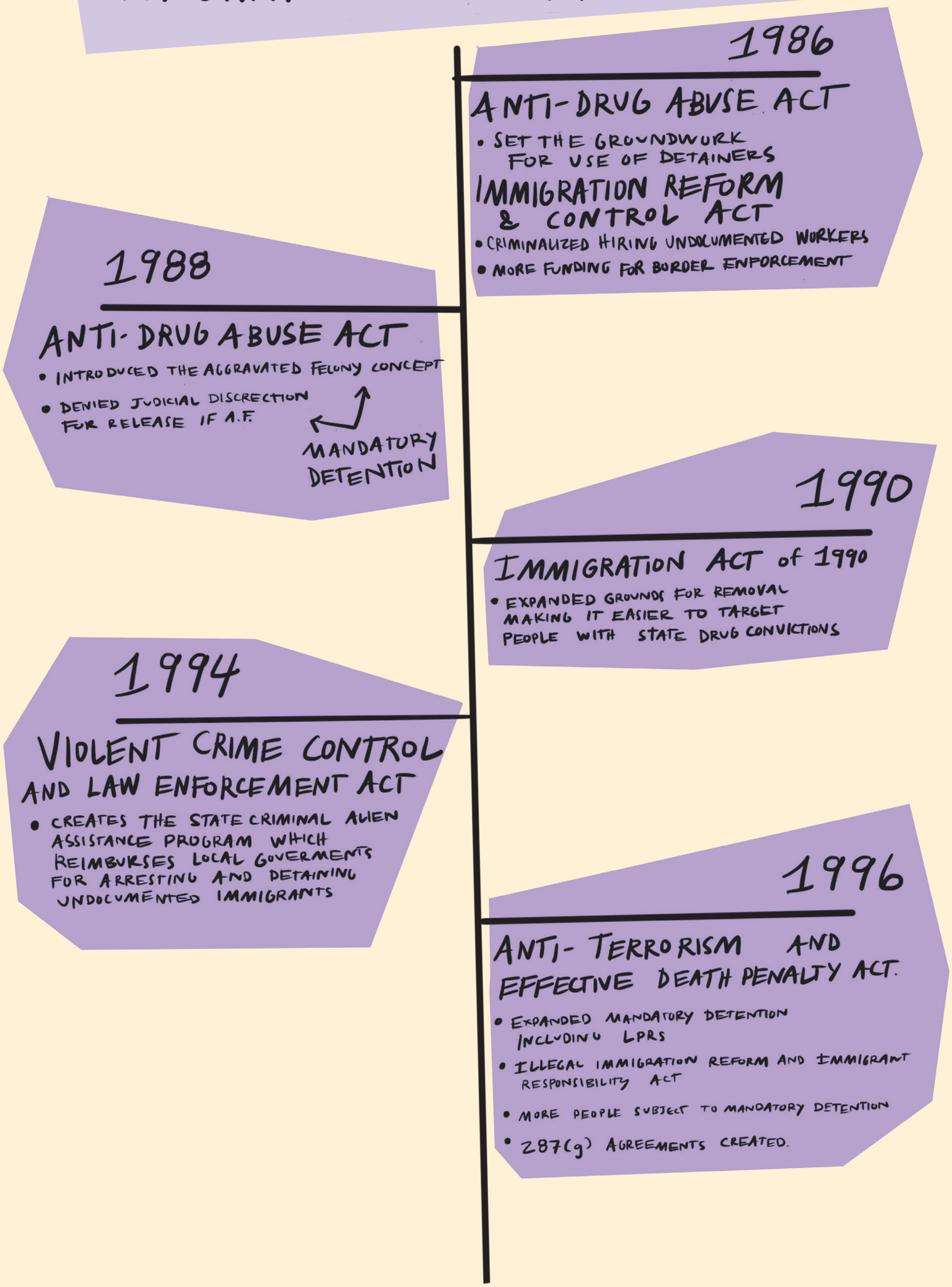
Image Source 2

Digitization and centralization of government databases began as early as 1967 with FBI records.[3] However, the digitization of migrant records came much later. It was not until 2008 that fingerprints accompanying applications for immigration "benefits" like travel visas and naturalization were uploaded, and 2010 when ICE investigators began consistently uploading fingerprints taken from people during law enforcement encounters.[4]

> "The legal architecture of modern US immigrant criminalization is less than forty years old."

Many key laws have roots as recent as the 1980s, when the Cold War and the racialized War on Drugs collided. In 1986, the Immigration Reform and Control Act (IRCA) criminalized hiring undocumented workers for the first time in US history, and increased resources for the INS to patrol the border.[5] IRCA also mandated the US Attorney General to deport noncitizens convicted of "removable offenses" as quickly as possible. This began the practice of targeting immigrants convicted of crimes and expanded the mechanisms for policing immigrants.

MODERN LEGAL ARCHITECTURE of MIGRANT CRIMINALIZATION



1986

ANTI-DRUG ABUSE ACT

- SET THE GROUNDWORK FOR USE OF DETAINERS

IMMIGRATION REFORM & CONTROL ACT

- CRIMINALIZED HIRING UNDOCUMENTED WORKERS
- MORE FUNDING FOR BORDER ENFORCEMENT

1988

ANTI-DRUG ABUSE ACT

- INTRODUCED THE AGGRAVATED FELONY CONCEPT
- DENIED JUDICIAL DISCRECTION FOR RELEASE IF A.F.

MANDATORY DETENTION

1990

IMMIGRATION ACT of 1990

- EXPANDED GROUNDS FOR REMOVAL MAKING IT EASIER TO TARGET PEOPLE WITH STATE DRUG CONVICTIONS

1994

VIOLENT CRIME CONTROL AND LAW ENFORCEMENT ACT

- CREATES THE STATE CRIMINAL ALIEN ASSISTANCE PROGRAM WHICH REIMBURSES LOCAL GOVERMENTS FOR ARRESTING AND DETAINING UNDOCUMENTED IMMIGRANTS

1996

ANTI-TERRORISM AND EFFECTIVE DEATH PENALTY ACT.

- EXPANDED MANDATORY DETENTION INCLUDING LPRS
- ILLEGAL IMMIGRATION REFORM AND IMMIGRANT RESPONSIBILITY ACT
- MORE PEOPLE SUBJECT TO MANDATORY DETENTION
- 287(g) AGREEMENTS CREATED.

Source [6]

The Clinton administration continued and expanded those practices, passing the Antiterrorism and Effective Death Penalty Act of 1996, or AEDPA, which created and expanded the grounds for mandatory immigrant detention and deportation, including for long-term legal residents. It was the first US law to formally authorize fast-track deportation procedures, a modified form of which is widely used today.[7]

Additionally, the Clinton administration passed the Illegal Immigration Reform and Immigration Responsibility Act (IIRIRA) in 1996, which conflated immigration and criminality.[8] IIRIRA is a keystone of our current immigration policy. It:

1. enabled the creation of the 287(g) program, which allowed DHS to enter into agreements with local law enforcement to perform certain functions of immigration agents;
2. expanded the list of convictions that trigger "mandatory" detention; and
3. increased the number of convictions that trigger deportation by further expanding a category applicable only to immigrants that was created by the Anti-Drug Abuse Act of 1988: "aggravated felonies.[9]

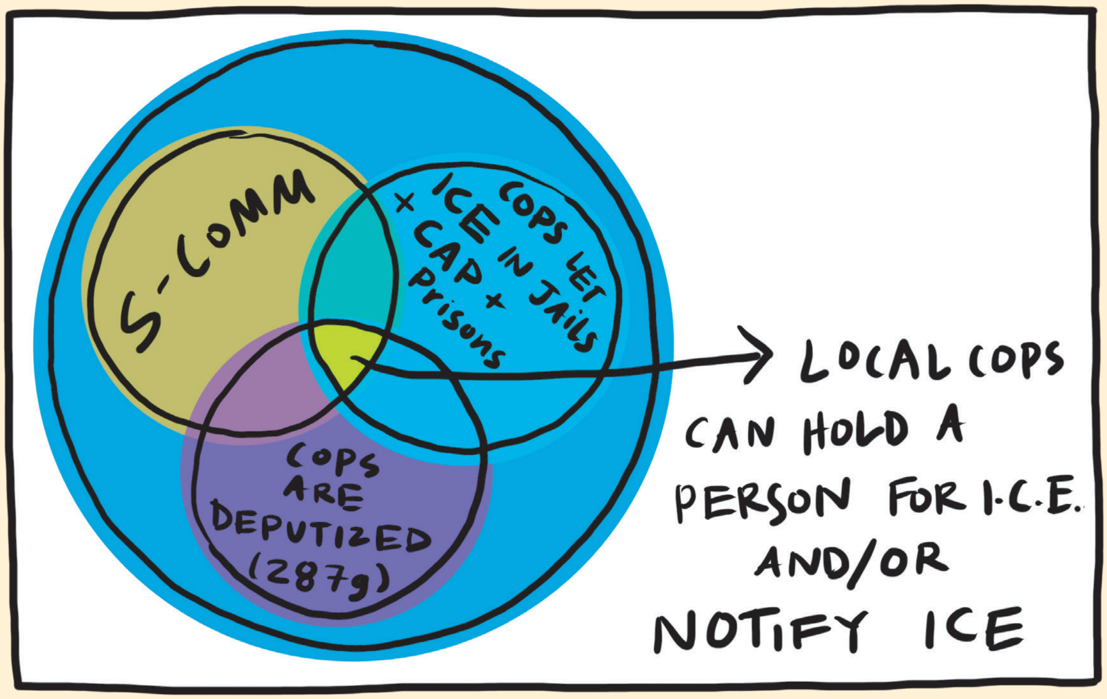
Congress determines which offenses qualify as aggravated felonies (not all aggravated felonies are felonies), and an aggravated felony conviction precludes access to relief like asylum and increases vulnerability to deportation.

POLICE + ICE COLLABORATION

In the following section, we look at three notable police-ICE partnerships that institutionalized data criminalization of migrants and non-citizens within non-immigration law enforcement protocols.[10] As we will see, systemic information-sharing at the data network level nullifies many of the sanctuary agreements that are in place today.

Formal FBI and DHS database integration is even newer than the crimmigration laws named above, dating back to around 1998. It accelerated following the 2001 Patriot Act, when Congress mandated the creation of an electronic system to share law enforcement and intelligence information to confirm the identities of people applying for United States visas.[11] At the same time, Congress restructured federal law enforcement laws to conflate "national security," "crime control," and "immigration control."[12] Just one year later, in 2002, Congress created DHS and granted it immediate access to information in federal law enforcement agencies' databases, sealing the deal for an interlocking web of automated database sharing.

Various programs since the 1980s had already given immigration authorities access to police data, jails and prisons. These programs often do not have clear beginning and end dates. There are implementation differences based on region, and there are overlaps and inconsistencies. Furthermore, in response to public pressure opposing formal law enforcement collaborations with ICE, the agency continued its information-sharing collaborations with local and state law enforcement — but often under the radar. Today, much data-sharing and immigration status-querying is built into the computer systems used by law enforcement to perform routine functions (like uploading someone's fingerprints). Under the current automated systems, every single person who was born outside of the US — or whose birthplace is unknown to US government databases — is automatically scrutinized for deportation if they are arrested and booked for anything, regardless of the charge and whether it is ultimately dismissed.[13]


S-COMM
COPS LET ICE IN JAILS + CAP + PRISONS
COPS ARE DEPUTIZED (287g)
LOCAL COPS CAN HOLD A PERSON FOR I.C.E. AND/OR NOTIFY ICE

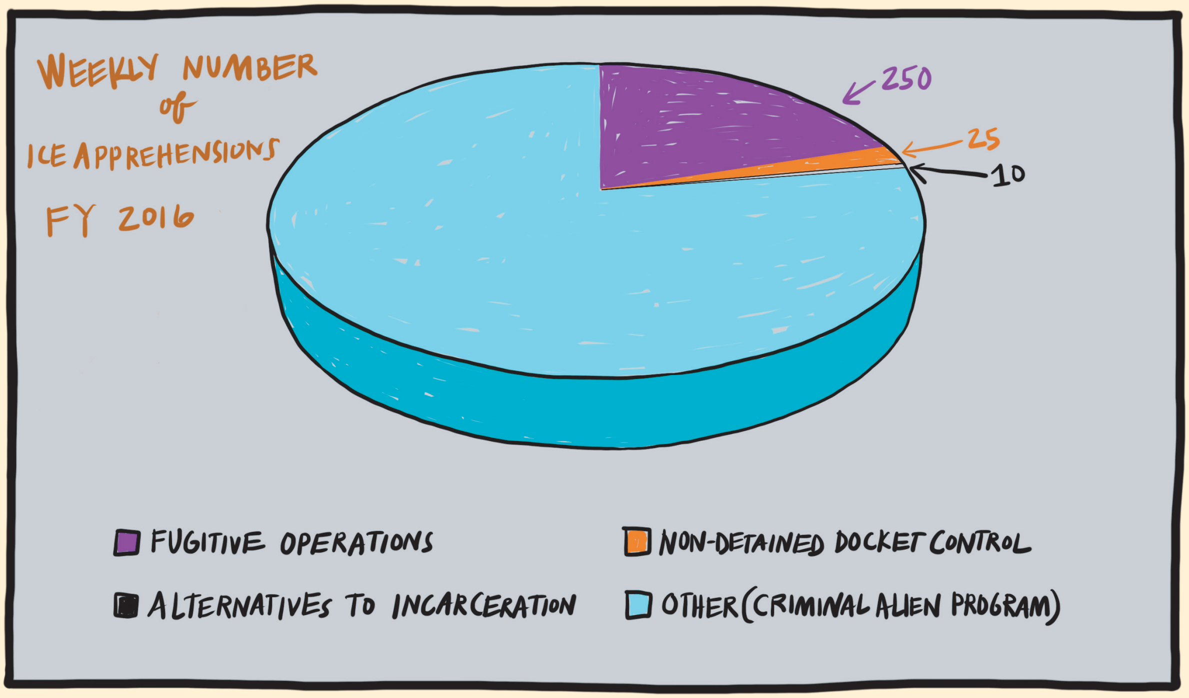
CRIMINAL ALIEN PROGRAM

The Criminal Alien Program (CAP) has been around in one form or another since a 1986 law decreed that people convicted of certain crimes should be an enforcement priority. CAP has been more aggressive in some states than others. "The unevenness in the program certainly implies that the preferences of state and local law enforcement officers (as well as the preferences of ICE agents in one region or another) played a role," a Vox article stated.[14] Today, CAP is an umbrella program that includes a variety of local law enforcement and ICE partnerships with names like VCAS, LEAR, REPAT, DEPORT, JCART, which use tactics ranging from in-person "jail checks" to automated biometric database-sharing.[15]

CAP began as mostly low-tech, voluntary collaborations between local law enforcement and immigration enforcement. Under CAP, jails and prisons often shared booking records with immigration agents and/or allowed immigration agents in-person access to interrogate incarcerated people ICE suspected it could deport — regardless of whether the booked person could eventually be charged or convicted.[16] CAP allows local cops to funnel people directly into ICE's custody, and allows ICE to use the criminalization process as a tool to facilitate mass deportations. CAP absolutely is premised on racial and national origin profiling and targeting: If you are a "suspected noncitizen," that is enough to qualify you for a CAP screening and ICE interrogation in jail or prison.[17] A 2013 American Immigration Council report found that CAP screens "all self-proclaimed foreign-born nationals found within Bureau of Prisons (BOP) facilities and all state correctional institutions."[18]

Despite its name, CAP programs were used to deport more than 22,000 immigrants without criminal records between FY 2013 and FY 2016.[19]

CAP was in place long before S-Comm was piloted in 2008 (more on S-Comm below). It operates out of all ICE field offices, in all state and federal prisons, and many local jails. [20] It has blended seamlessly with S-Comm machinery and processes, as ICE makes use of many of the same automated database checks set in motion by law enforcement booking and heavily relies on cooperation from jails and prisons to honor detainers and requests for notification of release. During the Obama era, CAP was the primary mechanism through which ICE deported people from the US interior. [21] Vox reported that CAP was responsible for between two-thirds and three-quarters of deportations during the Obama era of the early 2010s. [22] TRAC at Syracuse University concluded similarly for FY 2016, based on analysis of case-by-case records on both apprehensions and removals data obtained from ICE in response to hundreds of Freedom of Information Act requests, appeals, and a successful lawsuit. [23]



Source [24]

Although CAP is still known by many as a "jail status screening" program, both CAP and S-Comm use automated systems (detailed below) that attempt to match to FBI files and immigration records biographical and biometric information taken from a person by a cop during booking. Historically, "biometrics" has generally meant fingerprints; today, ICE and the FBI are outfitted with facial recognition software and readily available photo data from state driver's licenses, visa and naturalization records as well as photos scraped from the Internet and social media.

287(G) AGREEMENTS

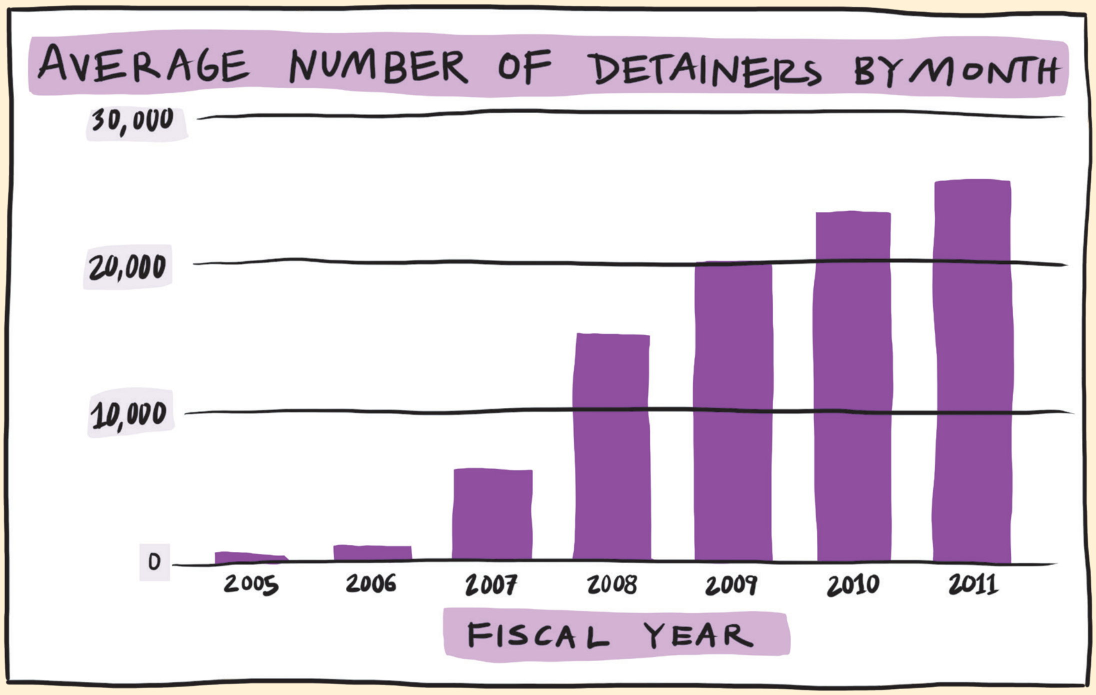
Section 287(g) of the Immigration and Nationality Act (INA) allows DHS to deputize state and local police to carry out federal immigration enforcement through interrogations and arrests, or following resolution of local, state, or federal charges. These partnerships today take two main forms: the "jail enforcement model," which authorizes local police to issue immigration detainers, or the "warrant service officer model," which ask jails or prisons to notify ICE, or hold a person for ICE, if a person is suspected of being deportable.[25] 287(g) partnerships are voluntary and formalized through MOU agreements made between state or local law enforcement with federal immigration authorities.[26]

The Trump administration dramatically increased the number of 287(g) agreements — from 34 at the end of 2016 to 151 as of November 2020. However, despite the increase in 287(g) agreements, it is difficult to calculate if deportations increased as a result. ICE claims that it does not break out 287(g) data to count deportations, and instead issues monthly reports of "encounters" that only include "a sampling" of people identified under the 287(g) program.[27]

SECURE COMMUNITIES (S-COMM)

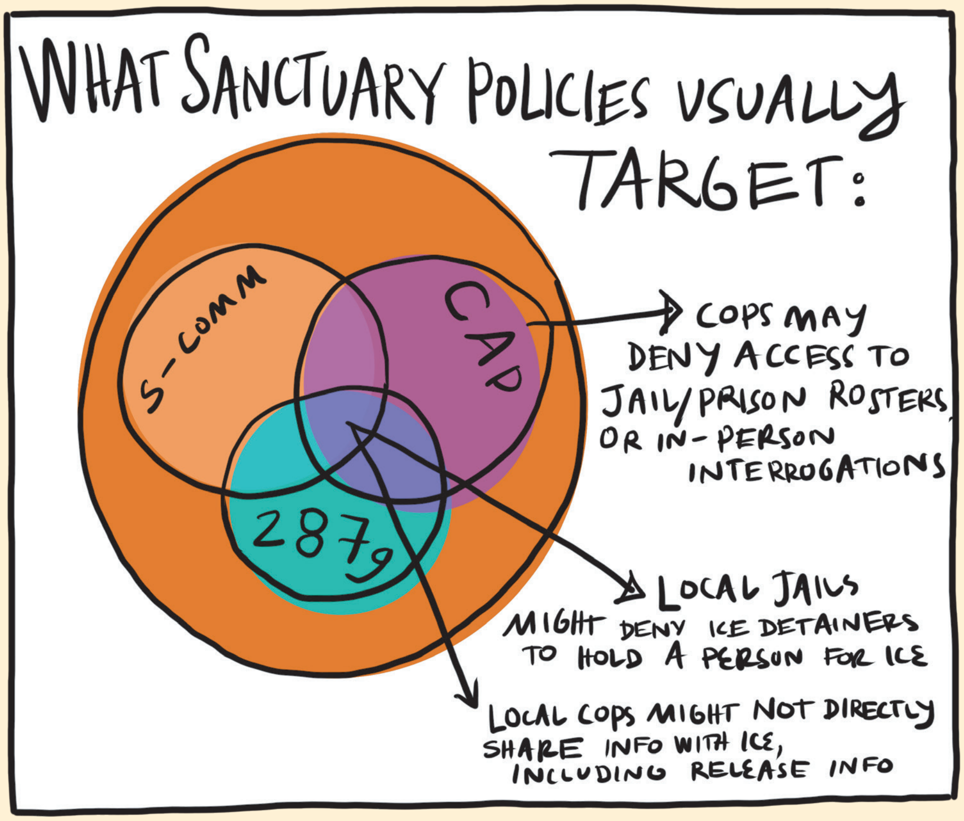
S-Comm was piloted by DHS in 2008. It formalized the now-ubiquitous automated process of forwarding fingerprints collected during law enforcement booking to check against immigration and travel databases for potential deportability.

Automating database checks had immediate and dramatic consequences. One product of ICE automation is the detainer (detailed below) — which has taken either the form of ICE requesting that a jail or prison "hold" a person who could be released, or a request from ICE for "notification of release" of a person whom ICE thinks might be deportable. In FY 2005, ICE issued roughly 600 detainers based on automated fingerprint matches per month — but by the end of FY 2011, monthly detainers exceeded 26,000. Although S-Comm was voluntary at first, following opposition from advocates and community members in New York, Massachusetts, and Illinois, the federal government mandated the program.[28] By January 22, 2013, S-Comm database sharing had been fully implemented in all 3,181 jurisdictions within 50 states, the District of Columbia, and five US territories.

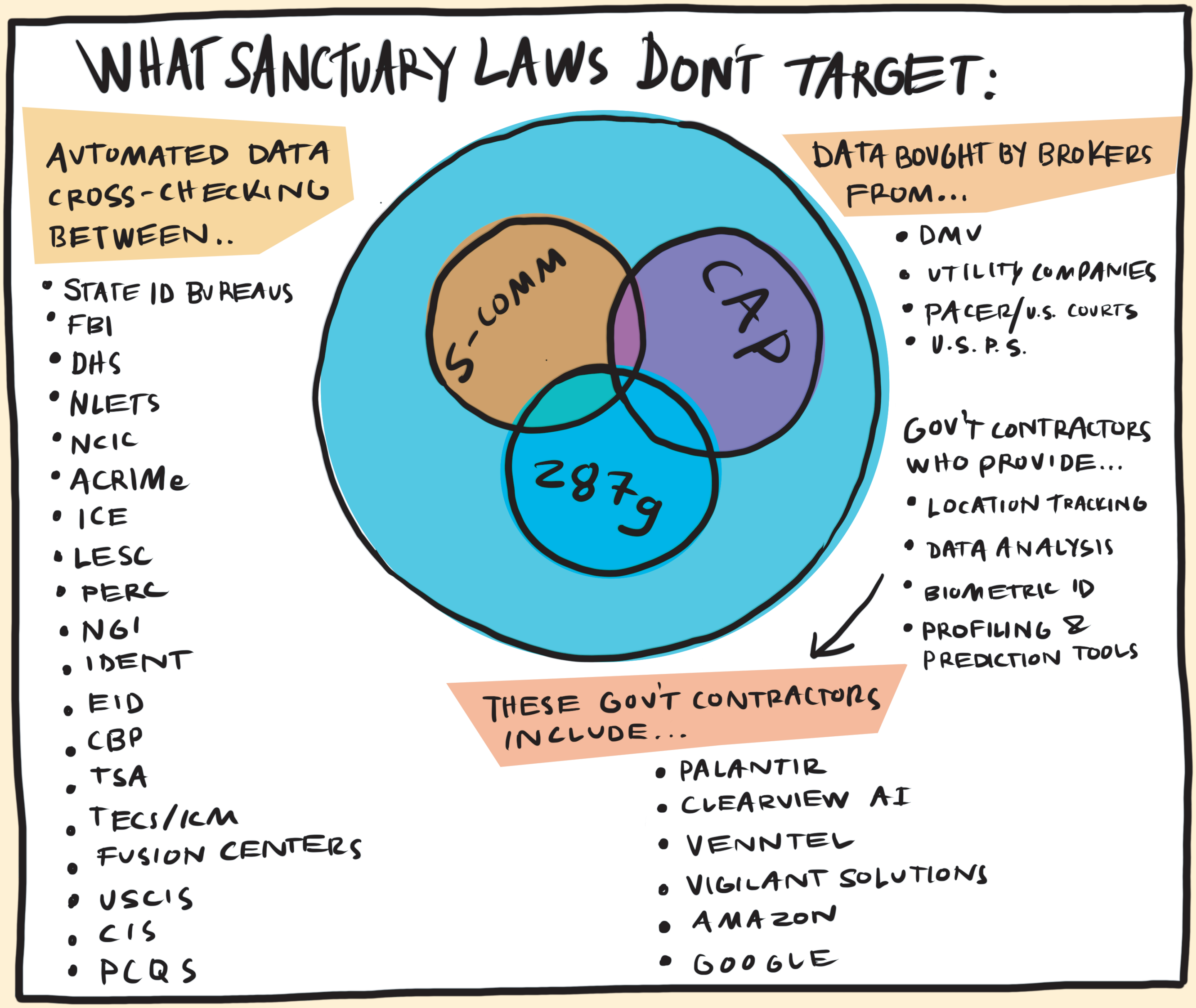


Source [29]

S-Comm generated much public backlash, and various communities have pressured their jurisdictions and Sheriffs to refuse to cooperate with ICE detainers. TRAC reported that "law enforcement agencies with the most recent recorded refusals were concentrated in New York and California," and two out of three detainer requests addressed to Queens and Brooklyn Central Booking were recorded as refused.[30] Santa Clara County in California refused to honor detainers over 90 percent of the time.


WHAT SANCTUARY POLICIES USUALLY TARGET:
S-COMM
CAP
287g
COPS MAY DENY ACCESS TO JAIL/PRISON ROSTERS, OR IN-PERSON INTERROGATIONS
LOCAL JAILS MIGHT DENY ICE DETAINERS TO HOLD A PERSON FOR ICE
LOCAL COPS MIGHT NOT DIRECTLY SHARE INFO WITH ICE, INCLUDING RELEASE INFO

S-COMM, CAP, 287g, WHAT SANCTUARY POLICIES USUALLY TARGET: Cops may deny access to jail/prison rosters or in-person interrogations, Local jails might deny ICE detainers to hold a person for ICE, Local cops might not directly share info with ICE, including release info



Laudable though these victories have been for organizers, especially at the local level, it is important to keep in mind that detainers are just the tips of those icebergs — and **if a person is not directly transferred to ICE custody from local law enforcement, there are still a number of ways that ICE is able to locate and control a person who is marked by criminalizing databases.**

AUTOMATED PROCESSES OF DATA CRIMINALIZATION

MIGRANT+TRAVELER STALKING
COMMERCIAL DATASETS
HSI + ICE
DATA CENTERS
ARREST + BOOKING
CONSTANT SURVEILLANCE + PREDICTION

How can we dismantle the entire system of data criminalization, which is fully automated at the database and computer level? Here, we take an in-depth look at two of these processes and data systems.

1. **Arrest and booking:** Database cross-checking with some DHS records became standard procedure in daily policing during the era of S-Comm implementation, but things didn't stop there. Today, criminal punishment data is merged with an expanding array of DHS datasets and commercially sold cell phone app, location and identification data for prediction and profiling purposes. Below, we detail a shortened version of this process, step-by-step.

2. **Travel surveillance and criminalization:** Well before S-Comm, and even before September 11, 2001, airline surveillance and Internet purchase spying was already a norm. Since 9/11, as we will see, the state has largely replaced its former "blacklist" model with algorithmic continuous trolling, creating and using AI to process massive amounts of data and to selectively target any chosen population. Section 7 describes historical and cutting-edge tools and techniques used to covertly identify people in public spaces as well as carceral ones, and match them to multiple private and public datasets in order to evaluate them for the ambiguous quality of "risk."

DETAINERS: CRIMINALIZING POTENTIAL

For those of us who are in contact with the immigration system, a detainer[31] or immigration hold (a version of Form I-247[32]) may be the first artifact we encounter in ICE's data criminalization process that follows a police stop. Detainers are requests by ICE for law enforcement to hold someone in jail or prison for up to 48 hours past the point when they would be released from custody, or to notify ICE prior to release. Some version of an immigration detainer has been used by the precursor to ICE, the INS, since at least the 1950s.[33] But it wasn't until S-Comm's launch in 2008 that issuance of immigration detainers skyrocketed.[34] S-Comm automated the process, which, combined with the massive legal machinery of immigrant criminalization and deportation that developed over decades, created the data criminalization dragnet that is in effect today.

Detainers cast a wide net, translating ICE's internal version of "probable cause" into an arrest and possible deportation by attempting to connect the biometric and data profile of a person to records kept by government agencies and commercial databases that show possibility of a visa overstay, entry without inspection, an open warrant, criminal conviction, previous deportation or any other factor that makes a person vulnerable to ICE arrest.[35]

For much of the last decade, ICE has relied heavily — ideologically and practically — on the detainer. In turn, the detainer relies on digital automated data cross-referencing. As an October 2020 Congressional Research Service report notes, "most ICE detainers are based on electronic database checks."[36]

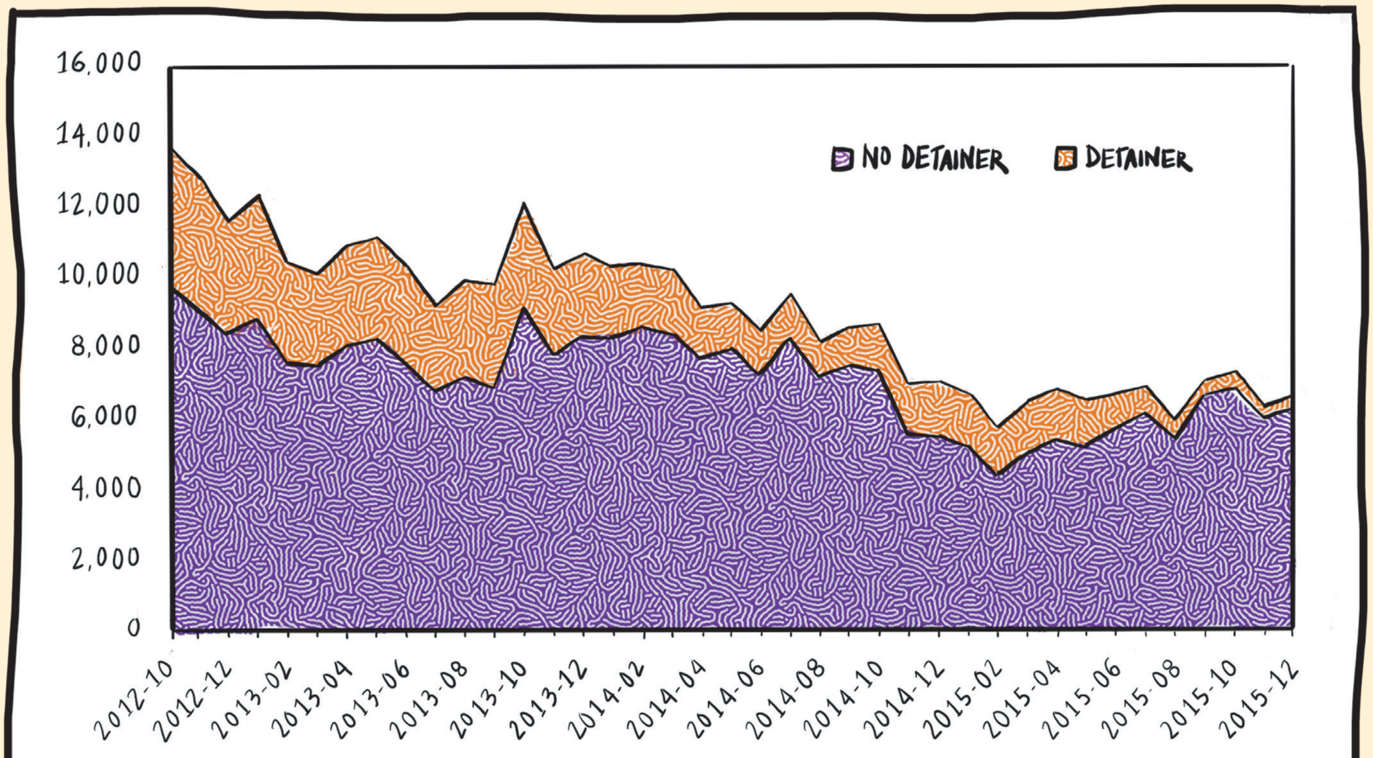
Using the detainer, ICE converts criminalized data into enforcement potential. By merging criminal and immigrant datasets, detainers purport to make real the longstanding claim that immigration is synonymous with criminality, and therefore, immigration and criminal enforcement are the same. But immigration detainers are not legally enforceable judicial warrants or official court "notices to appear;" they are just (legally questionable) requests from ICE to fellow law enforcement.[37]

NOT JUST DEPORTATION, BUT "INTEROPERABILITY" AND CONSTANT TRACKING

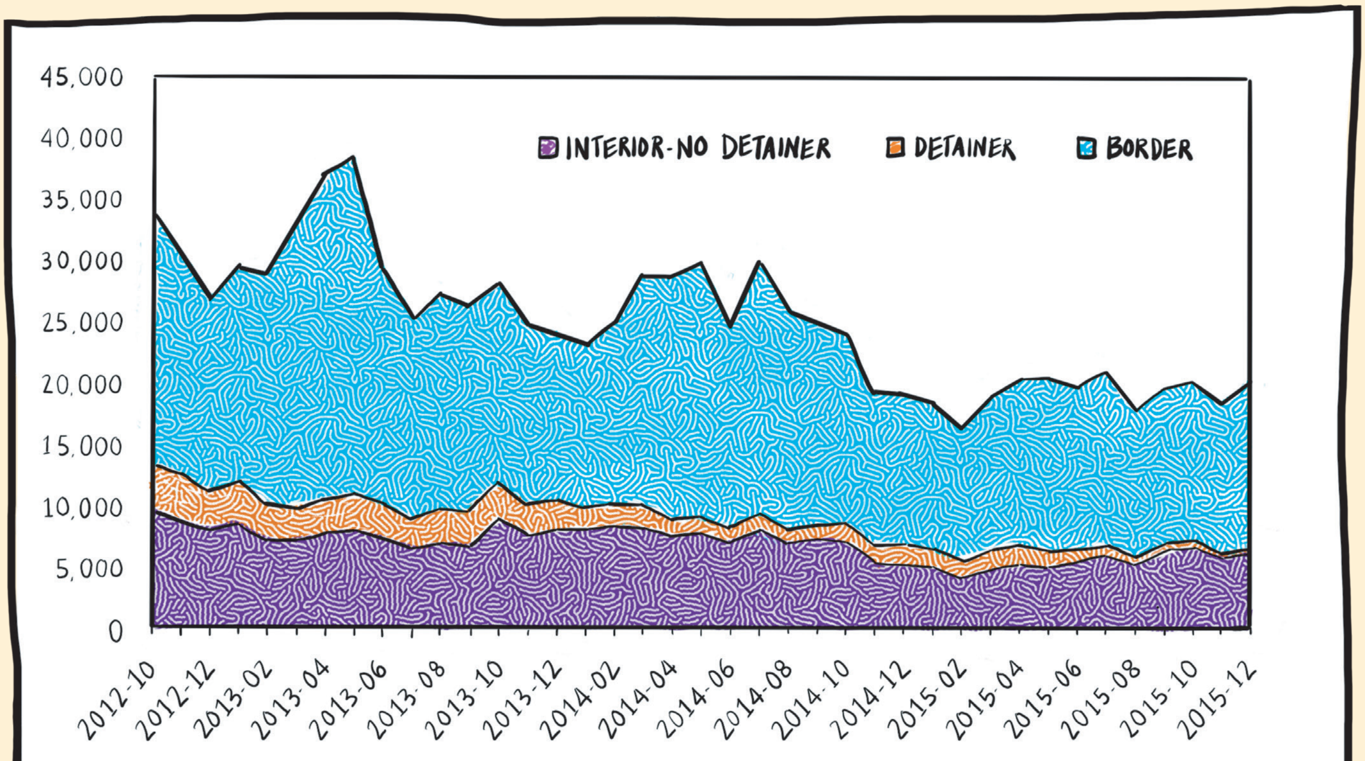
Detainers are not an endgame in and of themselves. They are visible iceberg tips that are part of automated processes that come downstream following multiple steps of data criminalization.

If we look at detainers alone, the story seems inconclusive. As noted earlier, in FY 2019 ICE did not take into custody up to 80 percent of the individuals for whom PERC issued immigration detainers.[38] These folks may still be located by ICE at their homes or upcoming criminal court dates for interrogation and/or arrest, but if they aren't, they may remain in limbo until a new event or encounter triggers the machinery of data criminalization once again.

Even amid peak deportations during the Obama era in 2013, S-Comm's fingerprint match-to-deportation ratio was at its highest, yet accounted for only around a quarter (28 percent) of ICE removals from non-border areas of the US, and less than 12 percent of all ICE removals.[39] Likewise, despite aggressive support for S-Comm by ICE under Trump, between 2016 and July 2017, only 2.5 to 5 percent of SComm deportations from the interior US were the result of detainers sent to local law enforcement agencies. TRAC noted: "When compared with ICE removals from all sources" — not just S-Comm fingerprint matches — "this component made up even a smaller proportion — less than 1 percent of all ICE removals."[40]



ICE DEPORTATIONS FROM INTERIOR & DETAINER USAGE



ALL ICE DEPORTATIONS & DETAINER USAGE

Source [41]

What the data suggest then is that detainers are not particularly effective as direct pipelines for the deportation of individuals, even those made vulnerable by the criminal legal system. It seems rather that the state's long game has been to establish a well-oiled "interoperable" machinery of databases that ensure that no matter who is in charge formally, a separate system — governed by targeting decisions, algorithms, and operating procedures — is able to expand and toggle between hidden, real-time, long-term tracking of individuals and high-profile, punitive enforcement intended to manage and criminalize communities of people based on the priorities of the moment.

> **"It seems rather that the state's long game has been to establish a well-oiled "interoperable" machinery of databases that ensure that no matter who is in charge formally, a separate system — governed by targeting decisions, algorithms, and operating procedures — is able to expand and toggle between hidden, real-time, long-term tracking of individuals and high-profile, punitive enforcement intended to manage and criminalize communities of people based on the priorities of the moment."**

UNDERMINING SANCTUARY

There are numerous ways that criminalizing data is passed between local and federal law enforcement agencies. Many of these automated processes negate and circumvent hard-won "sanctuary" policies. These processes fly under the radar, taking the form of short-lived pilot programs and informal agreements that can turn into unnamed and normalized long-term practices that are embedded in technology and may even contradict formal policies.

New York is one case study in confusion. Most people, including some politicians in the state, think that local sanctuary laws prevent police collaboration with immigration enforcement. But since database sharing is automated across all 50 states, there is no true way to opt out of "collaboration."

As the news site *Documented* reported, "New York state has a relatively robust sanctuary framework: only a single sheriff participates in the controversial 287(g) federal program, which deputizes local law enforcement officers — typically corrections personnel — to detain immigrants for questioning and arrests.[42] A New York appellate court ruled that local law enforcement cannot honor ICE detainer requests to hold immigrants in custody for longer than their normal release times.[43] Former state Governor Andrew Cuomo issued an executive order and amendment restricting state agencies' cooperation with ICE.[44]

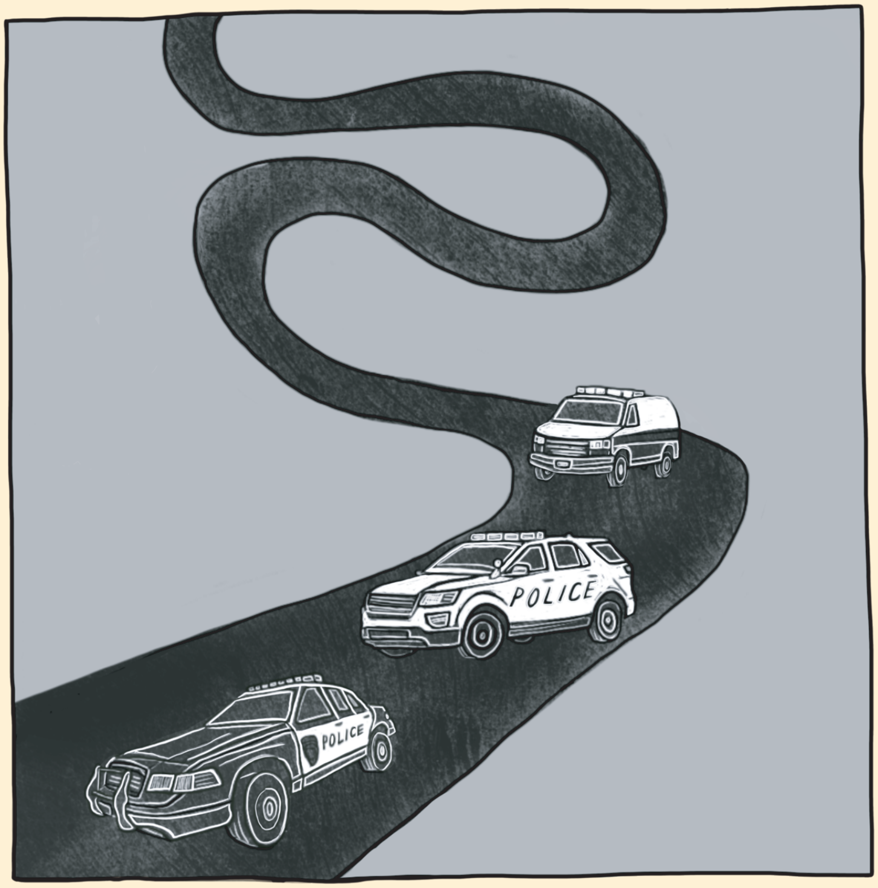
Yet, like every other US state, New York law enforcement officers and agencies use Nlets and NCIC, which pass on information (biographic or biometric) from everyone arrested for automated DHS database screening.

Separately, New York's Division of Criminal Justice Services (part of the State Identification Bureau) also receives booking fingerprints, and they send them to ICE as well. Since 2005, DCJS has specifically notified ICE every time it receives fingerprints of a person who has previously been deported. In fact, according to the state agency's 2009 annual report, DCJS would forward an electronic notice to LESC and a real-time Blackberry notification to ICE's New York City fugitive apprehension unit.[45] While the report and some of the technology described is old, the fundamental data-sharing structure is still in place. It remains DCJS policy to automatically forward a notification to ICE when a fingerprint taken by state authorities brings up a record that includes notice of a previous deportation. [46]

Similarly, since 2016 DHS' Law Enforcement Notification System (LENS) program has allowed local law enforcement (including campus safety officers) at agencies nationwide (not just in New York) to subscribe to email alerts that flag when a migrant leaving ICE custody is released in or intends to settle within that law enforcement agency's jurisdiction.[47] That is on top of ICE sharing that information directly with State Identification bureaus and fusion centers, who in turn can notify local law enforcement agencies.

HOW AUTOMATED CRIMINALIZATION WORKS:

Street-level harassment and arrest by police is disproportionately focused on working-class Black and Latinx people, and therefore tends to screen out non- or less-criminalized populations from immigration records searches, which are initiated after arrest when a person's fingerprints are booked. Once a person has their fingerprints booked, it is the discovery of any record that indicates foreign birth that triggers the IAQ and IAR process, which directs the weight of DHS inquiry and investigation onto that individual.[48] By structuring its computer systems in this way, non-immigration law enforcement and DHS have succeeded in procedurally and extra-legally implicating birth abroad, and even international travel, as criminalizing.



ARREST AND BOOKING

Two main, known procedural pathways for automated migrant criminalization are dubbed in the parlance of law enforcement's networked computer system the "Immigrant Alien Query" (IAQ) and "Immigrant Alien Response" (IAR). These are the computerized processes that automatically compare fingerprints collected by non-immigration police against DHS holdings in order to trawl an arrested person's records for evidence of foreign birth, travel visa applications, historical border-crossings and previous encounters with immigration enforcement. These records, if dredged up, subject an arrested person to new or reinvigorated scrutiny, surveillance, harassment and potential arrest by ICE.

As mentioned above, database cross-checking with some DHS records became standard procedure in daily policing during the era of S-Comm implementation and has grown to encompass many more datasets since. Here, we detail a shortened version of this process, step-by-step. In the appendices, we provide a much longer detailed description of each step of this process and the databases involved.

1. **You get stopped by a cop.** Maybe it is the result of a Stop-and-Frisk-type stop, or perhaps you were pulled over while driving a car with a broken taillight.

2. **The cop who stopped you demands your ID.** In some states, refusing to give your name to a law enforcement officer, or not carrying government-issued identification, can itself lead to arrest.[49]
   If you are carrying and hand over a US-issued ID or driver's license, the cop is likely able, using the information on the ID, to access almost immediately your DMV records that provide biographical details, information about whether your license is valid or suspended, vehicle registration, car insurance information, and home address.
   They, or a dispatcher, will also conduct a quick search for any open warrants that would show up in local, municipal and state databases.

3. **The cop may also decide to search your criminal history in additional federal databases.** They may be able to conduct this search from their car or via mobile device, or ask a dispatcher to do it for them.
   The databases they likely consult include: National Crime Information Center (NCIC) and Nlets

4. **You are arrested and taken to jail for booking. Your fingerprints are automatically checked against state-level and FBI files.** When your information and biometrics are loaded into the computer system, an automatic process is triggered. Your prints, photo, and biographical information are automatically forwarded to the State Identification Bureau (which are like FBIs at the state level that archive fingerprints and criminal history). Your biometrics are checked against FBI holdings, as well as the FBI's NCIC and Next Generation Identification (NGI) biometric databases.[50]
   Databases implicated: NGI and NCIC

ICE NERVE CENTERS: LAW ENFORCEMENT SUPPORT CENTER AND PACIFIC ENFORCEMENT RESPONSE CENTER

The Law Enforcement Support Center (LESC) and Pacific Enforcement Response Center (PERC) are two of a handful of ICE data centers that run 24/7 to follow as many leads as possible generated by the automated data criminalization process following a law enforcement encounter and database match. ICE claims that LESC workers process approximately 1.5 million biometric and biographic (IAQ) queries annually. Following a series of automated searches of at least sixteen visa, citizenship and criminal legal databases, the LESC analyst will recommend to an ICE deportation officer whether or not the person being searched may be removable, and whether a detainer, or immigration hold, could be issued.[51] LESC works closely with law enforcement and local Field Offices to provide information about people who are held in custody and whom ICE may be able to target.

5. **Nlets checks your biometrics against DHS' IDENT/ HART biometric database. If anything indicates that you might be foreign-born, your profile is forwarded on to ICE analysts via a biometric or biographic "Immigrant Alien Query," or IAQ.**

   If DHS has any biometric record of you in its massive database — which may have come from applications for an immigration "benefit" like a travel visa, naturalization or asylum [52] — then Nlets automatically creates a biometric "Immigrant Alien Query," or IAQ, which notifies ICE and law enforcement of the "match." Alternatively, a biographic IAQ is created if your biometric information cannot be matched to DHS' holdings, *but if you were born outside of the US* (or if DHS' records don't show where you were born).

   Both kinds of IAQ trigger a rapid and multi-step process created by ICE to automate the creation of detainers — a notice to law enforcement that ICE is supposedly investigating a person in law enforcement custody for violating immigration laws, and a request to notify ICE if that person is going to be released.
   Databases used: IDENT/ HART

6. **ICE analysts at the Law Enforcement Support Center in Williston, Vermont receive the IAQ from Nlets.**[53] IAQs are placed in a queue. Once an IAQ rises to the top of the queue, a contract analyst for ICE picks it off of the line, conducts cursory initial database queries, and begins working on an Immigrant Alien Response (IAR). The contract analyst uses a computer system, ACRIMe, and oversees the process of checking you against numerous government and private datasets.[54]
Databases used: Nlets and ACRIMe

7. **ACRIMe automatically searches for name and date of birth matches in various criminal, customs, and immigration databases.**[55]
Databases and systems used and searched can include: **ACRIMe, Nlets, CIS (Central Index System)**[56] **, CLAIMS 3 and 4, EID** (Enforcement Integrated Database), **EAGLE (EID Arrest Graphical User Interface for Law Enforcement) , ENFORCE, ENFORCE Alien Removal Module (EARM), Prosecutions Module (PM), OM², Law Enforcement Notification System (LENS), EDDIE, IDENT/HART, ADIS (Arrival and Departure System), SEVIS (Student and Exchange Visitor Information System)**, and **EOIR (Executive Office for Immigration Review)**

   Court documents from 2017 indicated that ICE relies on sixteen databases.[57] (This statement might downplay the fact that because many databases link to others, making contact with a system like EID may actually provide datasets from a dozen or more discrete databases.)

8. **Based on the above searches, ICE's data analyst at LESC decides whether ICE has the basis to issue a detainer or arrest you.** The ACRIMe user finalizes the Immigration Alien Response (IAR) that recommends to an ICE deportation officer whether you might be removable.[58] The IAR includes a person's last known immigration or citizenship status, basic biographical information and criminal history. ACRIMe then electronically returns the IAR to both the requesting agency and the ICE ERO Field Office that is in the region of the requestor. If the analyst decides that a person might be deportable, then an ICE agent or officer can lodge a detainer via the ACRIMe system, and the IAR is routed to the local ICE field office which has jurisdiction.[59] **Whatever the decision, an ICE field office can still carry out its own search, and has unchecked power to decide when the "evidence" it has is enough to justify a detainer or arrest.**[60]

9. **The IAR is sent from LESC to an ICE field office, and/or PERC.** ACRIMe allows contract analysts at PERC to search multiple criminal legal, DHS and commercial databases to cross-check for any possibility of deportability. ICE field officers can access the analyst's research via ACRIMe as well, and can also conduct their own research and investigation.

   PERC is a newer center, established in January 2015.[61] ICE contract analysts at PERC attempt to identify, locate, and build a case against people whom it suspects are deportable. This includes people who have been previously ensnared by the automated data criminalization system, but were released before ICE picked them up. PERC creates detainers all day and night, scraping datasets that collect everything from social media posts to family members' naturalization records to try to justify "probable cause" for a detainer.

   An ongoing lawsuit, Gonzalez v. ICE, called into question whether issuing detainers based on incomplete and inaccurate databases violates the constitution, and enjoined several states, temporarily preventing them from honoring PERC detainers. A Ninth Circuit ruling in September 2020 overturned the prior injunction, but as of February 2022, ICE agreed to honor the injunction voluntarily for a 6-month period (through August 2022) during settlement negotiations.[62]
Additional databases consulted by PERC analysts may include: **Commercial databases CLEAR and/or LexisNexis**

10. **ICE uses ACRIMe to issue a detainer to the jail where you are held**. Your fate is in the hands of your jailers.
Best case scenario: Even if the cops do not honor ICE's detainer, and you are released, your "permanent record" is now beefed up and freshly linked to criminalizing data. If you encounter law enforcement or immigration officials in the future, it will only take a quick database check for them to decide that you're worth detaining and investigating further. Also, ICE could decide at any time to prioritize coming for you. They have very updated information about where to find you.
Worst case scenario: If the jail decides to hold you or notify ICE about the details of your release, ICE could send over an agent to arrest you.