Digital Defense Playbook

Community Power Tools for Reclaiming Data

Contact Info

info@odbproject.org
https://www.odbproject.org
#OurDataBodies

Copyright Info

Suggested Citation: Lewis, T., Gangadharan, S. P., Saba, M., Petty, T. (2018). *Digital defense playbook: Community power tools for reclaiming data. Detroit: Our Data Bodies.*

TABLE OF CONTENTS

AUTHORS' LETTER

In order for us to understand and confront the ways in which data-based technologies are being integrated into our everyday lives and impacting our ability to self-determine and thrive, we must first understand how our communities—ones marginalized by race, class, gender, sexuality, immigration status, and other natural and imposed identities—are impacted by data-based technologies.

Our Data Bodies (ODB) has conducted research and produced a workbook of popular education activities focused on data, surveillance, and community safety to co-create and share knowledge, analyses, and tools for data justice and data access for equity. We hope that this project will be helpful to movements for justice grounded in peoples' realities. We hope that our work will enhance trusted models of community health and safety and help illuminate the differences between being safe and being secure. We wish this Digital Defense Playbook, with all its activities, tools, tip sheets, and reflection pieces, will support organizations and community members involved in intersectional fights for racial justice, LGBTQ liberation, feminism, immigrant rights, economic justice, and other freedom struggles, to help us understand and address the impact of data-based technologies on our social justice work.

This work is critical, because our data are our stories. When our data are manipulated, distorted, stolen, exploited, or misused, our communities are stifled, obstructed, or repressed, and our ability to self-determine and prosper is systematically controlled.

ABOUT ODB

ODB is a collaborative, participatory research and organizing effort. Since 2015, we have been working in three cities: Charlotte, North Carolina; Detroit, Michigan; and Los Angeles California. Our project combines community-based organizing, capacity-building, and rigorous academic research in order to find answers to three main questions:

- How do marginalized adults experience and make sense of the collection, storage, sharing and analysis of their personal information?
- How, if at all, do marginalized adults connect their ability to meet their basic material and social needs to their inclusion in (or exclusion from) data-based systems?
- What strategies do marginalized adults deploy, if any, to protect their digital privacy, self-determination, and data rights?

ODB was born from previous research and organizing in and around data profiling, data-driven technologies, resistance to surveillance, and digital justice. We grew from a set of shared interests: we wanted to shift who gets to define problems around data collection, data privacy, and data security—from elites to impacted communities; shine a light on how communities have been confronting data-driven problems as well as how they wish to confront these problems; and forge an analysis of data and data-driven technologies from and with allied struggles. We value principles of digital justice, which were first developed by the Detroit Digital Justice Coalition in 2010.[1] These principles celebrate the creation of spaces where people can explore technologies' power to investigate, illuminate, and develop visionary solutions to community problems.

1 *See Communication is a fundamental human right. Issue #2*, Detroit Digital Justice Coalition. Available at: https://bit.ly/2qm0JiB

Through our work, we aim to create a more just, peaceful, and equitable future for all people by:

- Conducting research that highlights the impact digital data collection and data-driven systems have on our human rights and local communities;
- Strengthening local communities and community organizations;
- Supporting community-defined problems and solutions;
- Inspiring a national conversation around the unique experiences of marginalized communities and data-driven technologies; and
- Uncovering how systems like open data portals, phone tracking, social media, social service databases, and predictive algorithms impact re-entry, fair housing, public assistance, community development, and people's overall ability to meet their basic human needs.

Our Cities

CHARLOTTE, NC

A beacon of the New South, Charlotte's population has transformed dramatically over the past century. As one of the country's most important financial centers, the city is undergoing dramatic demographic changes that include a forty percent increase in residential population over a ten-year period and growth in per capita income that outpaces that of the entire state.

However, Charlotteans do not reap the benefits of Queen City's booming economy equally, and these changes link to a longer history of gross inequities due to the displacement and forced labor of Black populations. According to a 2014 study, the city ranked last out of 50 large cities for income mobility. Skyrocketing rates of income inequality combined with segregation, mass incarceration, and the hollowing out of middle-class jobs have overwhelmingly contributed to the racialized disparities that exist now. While Charlotte holds a place in history books for its centrality in racial equality and civil rights movements, the severity of current-day racial disparities and the fierceness of residents fighting back now define the city.

DETROIT, MI

Once the industrial center and the fourth largest city in the United States, Detroit is a crucible of social transformation and participatory democracy, where residents—as the African-American folk saying goes—have been making a way out of no way for decades. For decades, and following the 1967 Detroit rebellion, subsequent radical demographic shifts from majority white to majority Black, and the election of the city's first Black mayor, Detroit residents have endured the weight of a dominant narrative that portrays them as "dumb, lazy, happy and rich." Following the 2014 election of

its first white mayor in 40 years, global perception of Detroit again shifted, with a new dominant narrative heralding the city's rebirth, again to the exclusion of Black residents and the realities of persistent inequities.

Residents have challenged the "comeback" narrative that largely focuses on corporate-led initiatives, especially the well-publicized decision of billionaire Dan Gilbert to move Quicken Loans, an online lending giant, to the downtown corridor of Detroit. Enthusiastic coverage of Gilbert's and other revitalization efforts neglects mention of the extraction of public resources, hi-tech surveillance of the downtown "Gilbertville," corporate fraud, and redlining practices leveraged by commercial actors against the residents of this majority Black city.

LOS ANGELES, CA

Los Angeles is the third largest metropolitan economy in the world and rates better than many other U.S. cities on scales of segregation and opportunity. Yet the annual count of people who are homeless saw a 25% increase in 2017.

And the wealth pouring into downtown is pushing out these residents, as gentrification replaces single residence occupancy (SRO) units with live/work lofts. A recent study found just nine usable toilets at night for a street-based population of almost 2,000, far below United Nations' mandates for human rights and cleanliness.

As marginalized communities push back—such as a drive for Skid Row to have its own elected neighborhood council—our work in Los Angeles considers resistance to surveillance, whether by police or other state actors such as the Department of Social Services. The Los Angeles Police Department's history of misconduct and abuse gives pause as the agency has developed some of the most sophisticated and secretive surveillance systems in the country. This includes a partnership with a CIA-backed company on the forefront of predictive policing and deployment of facial recognition software on parts of its vast CCTV network to search for "matches" to a closely guarded and problematic gang database.

Our Community Partners

The Center for Community Transitions, Inc. (CCT): An organization in Charlotte that is primarily focused on helping individuals with criminal records navigate paths towards healthy and productive lives.

The Detroit Community Technology Project (DCTP): An organization that uses and develops technology rooted in community needs, designed to strengthen human connections to each other and the planet.

Stop LAPD Spying Coalition (SLSC): A sponsored project of the Los Angeles Community Action Network (LACAN), SLSC is dedicated to dismantling government-sanctioned spying and intelligence gathering in all its forms. LACAN's mission is to help people dealing with poverty create and discover opportunities, while serving as a vehicle to ensure we have voice, power, and opinion in the decisions that are directly affecting us.

The Authors

Seeta Peña Gangadharan: A Filipino-Indian mother and research justice organizer, born in New Jersey and currently living and teaching in London.

Tawana Petty: A mother, anti-racist social justice organizer, author, and poet, born and raised in Detroit, Michigan.

Tamika Lewis: A Black Queer mother and community organizer focused on advancing Queer People of Color and marginalized communities towards liberation through the dismantling of capitalism and all its forms of currency.

Mariella Saba: A Palestinian and Mexican queer mother born and raised in Los Angeles, where she dedicates her life to community organizing, popular education, cultural work, and healing arts to collectively and creatively contribute to all life's interconnected liberation.

Additional Contributors

Virginia Eubanks: A writer, teacher, welfare rights organizer, and co-founding ODB member from Troy, NY.

Kim Reynolds: A master's student, freelance writer, community and arts organizer, and music lover sitting at the intersection of art, politics, community, and justice.

Additional Partners

New America (primary grant recipient) is a think tank committed to renewing American politics, prosperity, and purpose in the Digital Age.

London School of Economics and Political Science (LSE) is one of the foremost social science universities in the world.

And Also Too is a collaborative design studio for social justice visionaries.

Our Funders

This work is made possible in part by a grant from the **Digital Trust Foundation (DTF). DTF** was set up by Facebook after Facebook lost a class action lawsuit. DTF funds projects that promote online privacy, safety, and security.

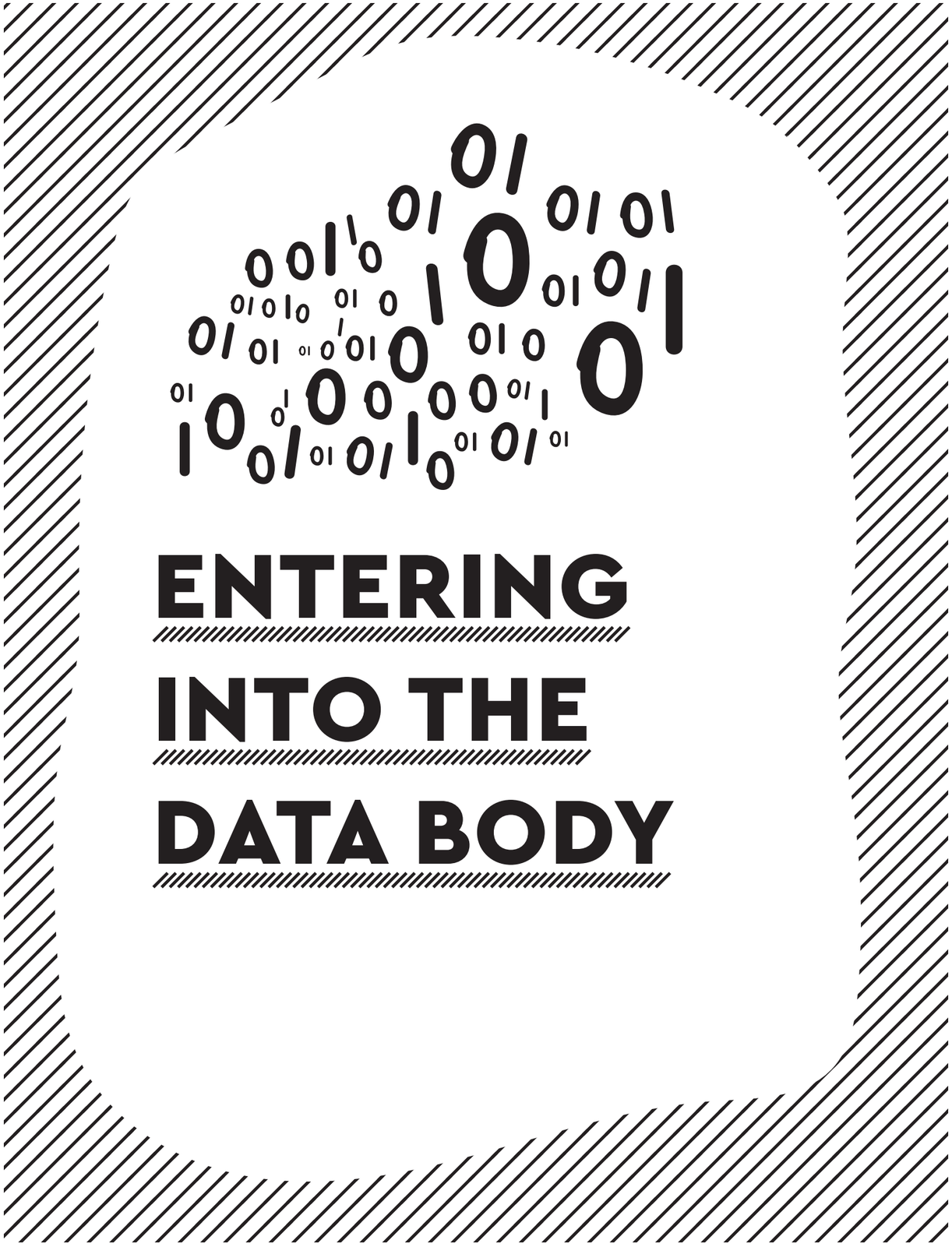
We are also thankful for support from the **Department of Media and Communications at the London School of Economics and Political Science**, the **Institute of International Education,** the **Media Democracy Fund**, and the **Mozilla Foundation.**

Acknowledgments

We are grateful to staff at the Center for Community Transitions, the Detroit Community Technology Project, and the Los Angeles Community Action Network (SLSC's organizational home), and Stop LAPD Spying Coalition. In particular, we want to thank Myra Clark (CCT), Diana Nucera (DCTP), and Hamid Khan (SLSC) for welcoming ODB into these organizations and for their leadership.

We would also like to thank Maurice Emsellem, Ames Grawert, Matthew Menendez, Aaron Rieke, Amy Traub, and Harlan Yu for reviewing our info sheets.

We would also like to thank Shakira Clarke, MSW, who gave us permission to include definitions from the Melanin & MagiQ Workbook, in "Commonly Used Terms." Thanks also to Tamika Lewis, for allowing us to reuse and/or adapt language in the "Using Digital Defense Playbook," "Facilitators' Roles," "Expectations for Group Facilitators," and "Group Norms and Agreements."



Using the Digital Defense Playbook[2]

SESSION LENGTH: The Digital Defense Playbook (DDP) can be facilitated as a series of community-based workshops or as individual, stand-alone workshops. Each session is developed to run from between 45 and 90 minutes and, if possible, can be successfully implemented in a 2-hour window of time. It can be restrictive for participants to share thoughts and ideas in less than 45 minutes, as these topics are complex, and we want to ensure that we are leaving our community members with a sense of power, not paranoia. Be sure there is uninterrupted access to a room for the activities to take place. Make reservations ahead of time, if necessary.

PARTICIPANTS: DDP activities, tools, and tips are designed primarily for People of Color (POC) and members of other marginalized communities, including poor, trans Queer, unhoused, and previously incarcerated people, as the activities were developed directly out of the stories and experiences of these same communities. At the same time, this guide can be used in any community. We do recommend organizers be mindful of protecting the group's safety and vulnerability, where necessary, in order to grow and maintain trust for session participants. These spaces are designed to allow our community members to speak uncensored about their experiences with racism, oppression, violence, and other forms of systematic violence without the fear of being silenced or overshadowed by others with greater privilege.

CHECK-IN AND ONE-ON-ONES: Community members may have to check-in with a facilitator if they are processing an experience or if they have been emotionally triggered by the conversation during group. Remembering that DDP activities are informed by facilitation principles for brave spaces, it is still important to hold space for folks who need to process more deeply. This may be the first time that our community members are addressing their experiences or realizing how impactful data collection and digital surveillance have been on their lives—honor that experience, have grace to allow for these experiences to be spoken and shared. The most important thing is that our community members start the process of healing if needed.

EVALUATION AND FEEDBACK: Using general feedback after each session is helpful for facilitators to evaluate if outcomes are being reached and that our community members are not left feeling disempowered. Session feedback forms can be distributed and collected after each of the sessions, and we also have included prompts in this guide. (See "Evaluation," p.93.)

2 The language in this section as well as "Facilitators' Roles," "Expectations for Group Facilitators," and "Group Norms and Agreements" were adapted from *Melanin & MagiQ* and Creativity2Day workshops. See https://bit.ly/2PIpmo5 and https://bit.ly/2Qo5gfU

Facilitators' Roles

MODERATOR

Facilitators should encourage discussion among the community members, not lead it. Keep the focus on the experiences and ideas of the group. If the conversation stops, the facilitator may choose to spark new conversation by asking new open-ended questions. Silence can be an advantage as it gives participants time to think and empowerment to speak. Include quieter community members by asking them directly if they would like to share on the topic. It is always okay for individuals to participate internally.

INFORMATION & EXPERIENCE SEEKER

Ask for facts, information, experiences, ideas, and feelings from the participants to encourage and build group discussion. Be mindful that any facts, information, opinions, and ideas that are expressed are also respectful of group norms and expectations (i.e., supportive & appropriate).

SUMMARIZER

Pull together related ideas or suggestions and restate or summarize the major points discussed. This can be particularly helpful after a lengthy discussion or as a means of focusing the conversation when talk becomes heated or off topic. You may relate some of the points made back to the goals you have established for the group. However, pay attention to new points or themes that arise.

ADDRESS CONFLICT

Pay attention to sources of difficulty or conflict within the group. Utilize group rules to keep the group respectful and supportive. Conflict in itself is healthy and a sign that change may be occurring. However, conflict should be mediated, and it is the role of the facilitator to maintain a respectful, safe, and supportive environment for that change to be beneficial to all participants.

SELF-CARE

The energy and enthusiasm you bring to the group helps bring out energy from participants. Prepare yourself before facilitating the group by nourishing your body, dressing comfortably, and coming prepared at least 30 minutes before facilitation. These conversations can be just as hard on facilitators as they are for community members. Take time before and after facilitation with your co-facilitator(s) and/or trusted friends to help process your own experiences in relation to the topics of this Digital Defense Playbook.

Expectations for Group Facilitators

BE AFFIRMING: Offer encouragement and positive feedback towards the participants with each facilitator making the effort to affirm at least one of the participants during a group session.

EXERCISE EMPATHIC LISTENING: Be mindful of not giving in to the pressure of always having to continue the discussion by speaking and being more intuitively attentive to what participants are sharing.

FACILITATE, DON'T LEAD: Facilitators are members of the group who help structure the discussion and keep it moving. Facilitators should not monopolize group time or stifle the discussion unless it becomes inappropriate.

BE FAIR AND IMPARTIAL: Facilitators should mediate disagreements, but not encourage or discourage any one "side." Try to separate the statements of a person from their personhood. People have a right to their own opinion.

PROHIBIT HARMFUL LANGUAGE: The facilitator should maintain a safe and supportive environment in the support group at all times. The use of sexist, homophobic, transphobic, racist, ageist, or otherwise disparaging or limiting language should be discouraged. If the facilitator believes that a person is using this language or behavior, they are responsible for addressing this in an educational and supportive manner.

KNOW YOURSELF AND BE YOURSELF: Be confident and fully prepared. It is okay to be a little nervous. If anything, you will be a lot more alert towards what is going on. Allow yourself to laugh, to have a sense of humor, and at times even to cry. There may be moments when you will not be able to stop yourself from becoming emotional. Ideally, you should be able to look at the subject matter and anticipate such a possibility. Whether you expect this to happen or not, keep in mind that it is still your responsibility to maintain focus and continuity on the subject.

KNOW YOUR SUBJECT MATTER: It will be extremely helpful to study your topic beforehand, especially if you yourself do not have personal experience with the kinds of circumstances in question.

KNOW YOUR AUDIENCE: Respect them and listen to what they say. Call them by name if you are able.

BE LIVELY AND ENTHUSIASTIC: Exuding more energy will increase the engagement of participants in discussion.

BE ORIGINAL AND CREATIVE: There are a million ways to express any single idea. Most of the time, you will have to choose one. You can build suspense, use analogies, and metaphors to convey complex themes, and employ parallelism to relate two seemingly opposing viewpoints. This will challenge what the participants believe.

VARY YOUR VOCAL QUALITY AND MAKE STATEMENTS CLEAR, SIMPLE, AND EASY TO REMEMBER: Changes in pitch, speaking rate, and volume will prevent you from sounding monotonous. Offer ideas one at a time and relate them to each other. Summarize when needed.

USE YOUR BODY BETTER: If your gestures, body posture, and facial expressions are meaningful and even genuinely animated, they will help show participants that what you are saying is important and that your engagement is a reflection of your commitment to the group's purpose. You can also use body language to help direct the flow of conversation.

BE FLEXIBLE AND ADAPTABLE: Try to read and interpret verbal and non-verbal responses. This will allow facilitators to adapt the discussion more closely towards the needs of the participants. Allow the conversation to center on a topic if participants request—if a major action, event or politics are at the forefront of the minds of the group, move the group to process together. The session can always be run at another time.

PREPARE AND OVER-PREPARE: Always prepare more material than you think you will need. Time flies when you're having fun, so it is important to have enough activities, conversation starters, discussion points, etc., to accommodate for the progression of each group discussion.

KNOW THE LANGUAGE: The sessions in this Playbook refer to concepts, terms and cultural references which require the facilitators to be knowledgeable and clear about definitions. These concepts and terms are listed out in the section called, "Commonly Used Terminology" (p.19).

PLAN AHEAD FOR INTERPRETATION: It is crucial to have interpreters to ensure that everyone in your group understands and participates. A healthy and responsible practice is that the ones facilitating do not interpret the sessions. While organizing the workshops/activities, plan for interpretation with a language justice framework in advance. As a facilitator, this means having a clear assessment of who will be participating and what languages they will be speaking.

Group Norms & Agreements

These are the group norms we established for community-based workshops and programming. It is the role of the facilitator to uphold these agreements and remind participants what they agreed to if these norms aren't upheld. Feel free to use these, invite participants to build on them as desired, or create brand new ones all together.

RESPECT THE SPEAKER: If a person is sharing, allow them to share their complete thoughts, avoid interrupting them, and listen actively.

MOVE UP, MOVE UP: If you are someone who speaks often, move up to listen more. If you are someone who prefers to listen, move up to speak out and share more often.

RESPECT YOURSELF, EACH OTHER, AND THE SPACE: This group honors personal identity and urges every member to do the same. These stories are yours, and you are your most authentic self. Put yourself first, but also remember to respect the shared space and the others who are alongside you.

LEAN INTO DISCOMFORT: The topics discussed in this Playbook may feel uncomfortable to talk about because of oppressions felt in in your everyday life. These workshops are designed to center, amplify, and honor the experiences of the communities and the members that are most impacted. ODB promotes the idea of a "brave space" in order to speak openly about our lives and experiences. We ask members for the willingness to lean into discomfort and operate on a foundation of learning. The emotions and feelings that may arise are normal and help enhance authentic conversations together.

SPEAK FROM "I" AND EYE: Share from your own experience and perspective. Don't assume the experiences of others and avoid making comments or generalizations about entire communities. Keep your shares focused on what you see, what you notice, and what you feel.

BE PRESENT: It can be easy to be distracted by digital devices and the environment, and we ask that every member makes an effort to push past distractions to stay present for every member in group.

BURN/ALOE/RECOVERY: If someone says something which is offensive to you or is harmful you can say "Burn."' The person who said the harmful thing can say "Aloe." This will open dialogue about what was said, how it impacted the person and then discover what can be done next time to avoid the language or action. This is "Recovery." It is also okay to quickly recognize what happened and move along if the person impacted requests. Remember that impact is often different from intention. Just because you "didn't mean it that way" doesn't mean you can ignore taking responsibility for the impact you created for another person.

SAY WHAT YOU MEAN: You don't have to censor or edit what you feel or say in this group. Don't worry about being politically correct or having the "right language" to talk about your experiences. You are always right.

CONFIDENTIALITY: What is said here, stays here. What's learned here, leaves here.

BE BOLD: Be YOU! This is the time to be your most authentic self! No one will tell you to be otherwise in this group. Honor your true self!

TRIGGER WARNINGS: If you want to share about an experience which could be triggering for other members, please preface your statement or story with "Trigger warning [insert topic]." For example: "This reminds me of an experience I had. Trigger warning intimate partner violence…" Leave time if anyone needs to excuse themselves. It is encouraged to lean into discomfort in these instances.

Key Aspects of DDP

When facilitating the different workshops and activities in this Playbook, you should remember that we have presented you with a structure that we have found to be the most useful based on reflective focus groups, soft launches, workshop facilitations, and community feedback. No matter if you are going by the script provided or rocking your facilitation your way based on community needs, we encourage you to cover the basic points in our structure to ensure your community members leave with a sense of power, not paranoia. We want to avoid people leaving an event feeling helpless and unable to identify ways to combat the issues or use tools they acquire to be able to fight back. The aspects are as follows:

Story Sharing: We start all of our activities with stories about ourselves, our communities, and our history. Sharing stories in relation to data collection, systems in our lives, and more is part of recognizing our collective experiences and strategies.

Whatchu' Know about Data: Starting from zero, no matter who is in the room or what the intended audience is, this section provides an overview of the subject, tool, or system the workshop is trying to address. Doing so will ensure everyone in the room is (mostly) on the same page and has the same educational or political grounding.

Data Body Check-Ups: Digital data collection and data-driven systems have a real impact on our community members, their families, and their lives. So start with participants. Let the participants lead the discussion with their experience and their attitudes towards the topic, and allow space for the issues to come up and be affirmed and addressed. They are the experts, and this section is all about checking in with them to see what their experiences are and how they are doing.

Power Not Paranoia: The activities in this section are designed to build community knowledge, defense, health and wellness, and collective organizing strategies for anti-surveillance, digital privacy, and safe and connected communities. Reclaim power from whatever or whomever harmed their power. If a lot of issues arise during these activities, it is always a good idea to stop and ask: "What are you doing to protect yourself?" or "What are some ways we can think of to keep ourselves, our communities, or our data safe?" These questions provide our community members with tools and tactics they can employ to reclaim their power from the stalker state. When ending sessions, remember to refer back to these solutions.

Community Defense Toolkit: We've found it very useful to have identified ways the community members can plug into the work and support the reclaiming of their narratives and data. Whether campaigns, tip sheets, media making, artistic work, or more, participants can connect to different action steps and mobilize their power.

Commonly Used Terminology[3]

ALGORITHMS: A sequence of steps for solving a problem (e.g., like a recipe); in digital terms, a set of computational or mathematical formulas that use data as their main ingredient, transforming these data (input) into desired outputs.

BACKGROUND RECORD (ALSO KNOWN AS RECORD OR CRIMINAL RECORD): A report or reports of your criminal justice history, which may or may not contain the results of criminal arrest, prosecution, conviction, acquittal, or dismissal.

CREDIT REPORT: A record of information such as your bill-paying history, length of your account with a company, any outstanding debt you have, any unpaid debts that have been registered with a court, any public record of having been sued, gone bankrupt, or failing to pay taxes (tax lien), and history of debt collection against you; it is used to determine your credit score.

CREDIT SCORE: A risk assessment tool used primarily by lenders. A high credit score means you are a low risk, are likely to get a loan or other service, and will have lower interest rates or more flexible terms of repayment. A low credit score could result in not getting a loan or other services, or paying more for such services. In other words, people with "bad credit" may be charged a higher interest rate for any kind of loan, or denied a loan altogether.

DATA BODY: Discrete parts of our whole selves that are collected, stored in databases, the cloud, and other spaces of digitally networked flows, and used to make decisions or determinations about us. They are a manifestation of our relationships with our communities and institutions, including institutions of privilege, oppression, and domination.

DATA-DRIVEN SYSTEM (ALSO KNOWN AS AUTOMATED SYSTEM): Automation can be defined as the introduction of technologies into social or organizational practices, which often leads to the reconfiguration or replacement of human labor. These systems can perform in (relatively) simple ways, such as matching names in a database, to complex ones, such as weighing hundreds of factors to determine whether someone should get a job.

DATA: Facts, details, statistics, or any information collected together for reference or analysis.

DATABASE: A collection of data. Databases can be analog, but today most databases are digital, and storage and access to this collection of information about people or things can be done electronically.

DIGITAL SECURITY: Tools and tactics we can use to protect our digital data and devices from anyone or anything that might want to harm or hurt us.

3 Many of the terms listed here were reprinted from Melanin & MagiQ Workbook, with permission of Shakira Clarke.

DRONE: Also known as an unmanned aerial vehicle or a machine-operated technology used for policing, military, and surveillance. Drones are also used for commercial purposes (e.g., delivery), recreation (e.g., photography), and scientific study.

IMPLICIT BIAS: The unconscious attitudes, stereotypes, and unintentional actions (positive or negative) towards members of a group merely because of their membership in that group. These associations develop over the course of a lifetime beginning at a very early age through exposure to direct and indirect messages.

INSTITUTIONS: Fairly stable social arrangements and practices through which collective actions are taken. Examples of institutions in the U.S. include the legal, educational, health care, social service, government, media, and criminal justice systems.

INTERNALIZED RACISM: The acceptance of negative attitudes, beliefs, ideologies, and stereotypes perpetuated by the white dominant society as being true about one's racial group, and oneself.

INTERSECTIONAL/ INTERSECTIONALITY: The interconnected nature of social identities such as race, class, and gender as they apply to a given individual or group, regarded as creating overlapping and interdependent systems of discrimination or disadvantage.

MARGINALIZED: Marginalized peoples are those kept from meaningful and dignified participation in social life.

OPPRESSION: Prolonged cruel or unjust treatment or control; cruel or unjust exercise of authority or power.

PERSON OF COLOR: A person who is not white. This can include, but is not limited to people who are Black, Asian, LatinX/Latino, Pacific Islander, Indigenous/Native American, African, Mexican, etc.

PREJUDICE: Favorable or unfavorable opinion, feeling about, or attitude towards a person or group, usually formed without knowledge, thought, or reason. It can be based on a single experience, which is then transferred to or assumed about all potential experiences.

PRISON INDUSTRIAL COMPLEX: A term used to describe the overlapping interests of government and industry that use surveillance, policing, and imprisonment as solutions to economic, social, and political problems.

PRIVACY (ALSO KNOWN AS DATA PRIVACY): A human right that respects the right of people, including their data, to be left alone or kept to themselves. Privacy is also considered to be culturally and historically defined, meaning that data sharing practices might be considered perfectly OK for one group but not at all appropriate for another.

RACE: A social construct of human categorization determined by shared physical characteristics, ancestry, genetics, and biology. These traits can include hair and eye color, bone and jaw structure, skin color, and more.

SCHOOL-TO-PRISON PIPELINE: A process through which students are pushed out of schools and into prisons. In other words, it is a process of criminalizing youth that is carried out by disciplinary policies and practices within schools that put students into contact with law enforcement.

SEXUAL ORIENTATION: A person's emotional, romantic, and/or physical attraction to other people.

STALKER STATE: The immense, widespread web of systems of information gathering, storing, and sharing between public and private entities, local, regional, national and international law enforcement agencies, corporations, individuals, and many more, working together to track, trace, target, and ultimately stalk community members and entire communities.[4]

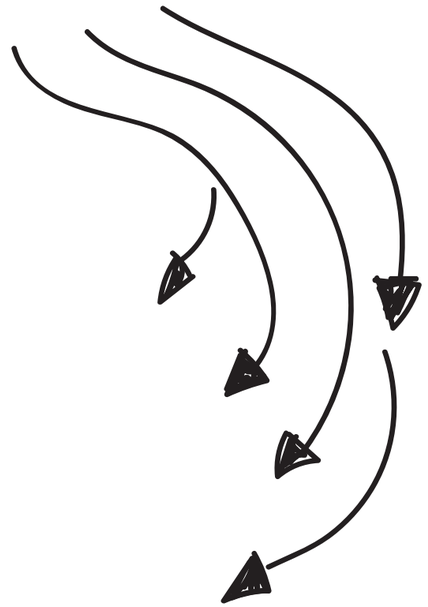
STEREOTYPES: Attitudes, beliefs, feelings, and assumptions about a target group that are widespread and socially sanctioned. Stereotypes support the maintenance of institutionalized oppression by seemingly validating misinformation or beliefs.

SYSTEMATIC VIOLENCE: Violence or harm that is directed at a particular social group, because of who that group is.

SYSTEMS OF OPPRESSION: The systematic mistreatment of people within a social identity group, supported and enforced by the society and its institutions, solely based on the person's membership in the social identity group.

TRANSGENDER OR TRANS: An umbrella term that describes a person whose gender identity differs from their gender assigned at birth.

WHITE SUPREMACY: A racist ideology based upon the belief that white people are superior in many ways to people of other races and that therefore white people should be dominant over other races.



4 See https://bit.ly/2QsfYSN for more information.

ODB Quote Bank

Below are quotes that reflect the ideas of community members we've spoken to thus far and that have helped to inform this Playbook. Community members were given the option to provide a pseudonym to protect their identity. Use these quotes with your community members to help open conversation about how data collection and data-driven systems are impacting our data bodies.[5]

"Each institution [should] deal only with the information it needs... Collection systems should only capture data that's necessary. They should not intimidate people. They should not violate their human rights."**—ANGÉLICA (LOS ANGELES)**

"Everything you do in this country, good or bad, it's used against you. Does it have an impact on your family? Of course it does! A very negative impact. Those who suffer most are always the children. What are we creating? Panic, fear, sadness."**—GUADALUPE (LOS ANGELES)**

"For their benefit they do communicate. But for my benefit, no."**—ASSATA (CHARLOTTE)**

"Harmful systems...try to separate. "OK, he's poor, he's rich." You are worth more because you are rich; you are worth less because you are poor."**—GUADALUPE (LOS ANGELES)**

"I don't think I've surrendered to the fact that they're just going to do what they're going to do."
—SAM (DETROIT)

"I had no option but to give it to them; I need to work, I need a cell phone to work, I need communication, I need a cell phone, so I had no alternative but to give out my information."
— UNA GUERRERA (LOS ANGELES)

"I have a criminal background. It's 15 to 30 years old. I plead guilty to worthless checks. It was 2003. Again, that's almost 15 years ago, but it's still held against me and it still hinders me. It makes it extremely hard to get employment, permanent employment. Basically, all of my jobs have been temporary positions or contract positions."**—JILL (CHARLOTTE)**

"I mean your face is not even your own anymore. Your face is being captured by cameras."
—DA HIVE (DETROIT)

"I mean, the credit score part, I really don't think that represents who I am, because first of all, I don't really even understand that. I understand that it needs to be at a certain level, but I just don't get why you need that. It's not necessary to me. I mean I'd rather have no credit than bad credit. I'm just saying, what is the point."**—NABRESHA (CHARLOTTE)**

5 Our interview questions are available on the ODB website.

"I really believe that every button that is pushed collects something about you."
—BEBOP (DETROIT)

"I think just mainstream society period is like once you have a criminal record, no matter if you stole bubblegum when you was 16, it's like you're a criminal. You're a bad person…"
—BONNIE (CHARLOTTE)

"I would love to un-Google my life!"**—ANONYMOUS (DETROIT)**

"I'm free in physical terms, but I wear a shackle around my ankle, so they know where I am, the places I go to, where I spend time, what places I've visited, so having that shackle is like having a spy over my shoulder, on top of me all the time, my whole life."**—VALERIA (LOS ANGELES)**

"It is important sometimes for us to also take stock and to recognize that even if we are the poorest and the least protected, even if we have made the worst mistakes, we have the right, the opportunity to love ourselves. Because we also have to. We have to keep our spirits up."
—MARCO (LOS ANGELES)

"It's out there. Once it's out there, it's out there. You can't take it back."**—CASSIDY (DETROIT)**

"Just like those telemarketers be calling. I don't understand how they get it if I'm blocking you and you still call back two or three days later. I think they scam it."**—J (CHARLOTTE)**

"Knowing your credit, knowing your scores, knowing how much you make, what you buy. So they can target you for giving a loan or not giving a loan. Deciding what you can have or not."
—JANET (LOS ANGELES)

"Like maybe there needs to be some protections on how corporations access data. Like maybe there's too much free reign."**—TACHALLA (DETROIT)**

"My cell phone is a prepaid cell phone. I don't have a contract, so there is no true tie back to my identity. Wherever I can minimize me giving someone any of my information, I will. I avoid as many contracts as possible. I do a lot of direct channel transactions if I can. I don't think there is anything that you can really do to secure yourself."**—RENITA GRAY (DETROIT)**

"No, I'm not feeling all that secure. Some of the way I'm feeling is because I don't fully understand the technology."**—SAM (DETROIT)**

"Nowadays, there are all these services where you can pay. Anybody can just pay a fee and get access to all kinds of information. It could be somebody who's stalking me. It could be somebody who—it could be a potential employer. I don't know even if it's legal, but who's going to stop them? They never have to tell me that they did it."**—JUSTICE BLACK (DETROIT)**

"I've sort of given up on trying to protect privacy."**—ANONYMOUS (DETROIT)**

"So, knowing that this electronic system that we live in has basically got us separated from the water that we need to swim towards in order to live, we're all struggling on the sands of the beach, trying to get back to the water."—**GENERAL JEFF (LOS ANGELES)**

"The worst thing I ever heard was, 'You probably should give up on finding a job.' He was like, 'I don't even know why you came today because you know you got a background, you know it's recent, and you know most places are not going to hire you so you probably should just stop trying. Go to school or something.'"—**KARRIEM (CHARLOTTE)**

"What's the price of me having my records expunged? After that, where do we go from here? You going to still neglect to forgive me, or you going to not forgive me? Is it going to count against other things I'm going to do in life to get ahead?"—**HATMAN (LOS ANGELES)**

"When applying for certain jobs, some of those websites share your information to colleges… which is uncomfortable. You're expecting a job-related call—an interview, and it's somebody asking if you want to go to college. It can be pretty forceful."—**JOHNNY D (CHARLOTTE)**

"When I slept on the curb I was confronted. They took pictures of me, but I didn't know they was taking pictures. I was covered up with a sitting blanket and the girl said 'They took your picture,' so he took the blanket off my head and said 'We're going to have to talk to you about [this] homeless, sleeping on the bus thing.'"—**DO (CHARLOTTE)**

"When you criminalize human behavior, and you criminalize human behavior of people for being people then you completely blur the lines as to the legitimacy of law and order."
—**BRAXTON (CHARLOTTE)**

"When you go to the DPSS [Department of Public Social Services] office they want to know all your information, if you own a house, if you own a car, if you own storage, if you own stocks...I mean how much money do you got in the savings account or do you have any money under your bed."
—**AMY BLACK (LOS ANGELES)**

"With social media, just be very privy as to what you keep on Facebook, make sure you're not putting your address or telephone number, any social security information on there."
—**(CHARLOTTE)**

ODB Themes

Below are themes that we have identified in our work with communities. Use these themes as a way of comparing how participants are making sense of and interpreting the larger impacts of data collection and data-driven systems, and how we and our interviewees make sense of their stories.

Security and surveillance. A feeling of being surveilled and insecure is a very real issue for some interviewees.

Predatory data systems. Interviewees express feelings of vulnerability in being exposed to systems they experience as predatory, biased, and exploitative.

Tracked and targeted. Many interviewees expressed feeling a lack of agency when interacting with data-collecting agencies, employers, and companies. This leads them to feel tracked and targeted by shadowy data systems.

Emotional and material costs. Interviewees have expressed fear, anxiety, and dread around the material consequences of data sharing.

My data doesn't represent who I am. People expressed concern and frustration about the unrepresentative nature of data collected about them and how it is used to profile them as they reenter society.

Systems are communicating but not for my benefit. Our interviewees agree that data-driven systems communicate with each other. Systems are integrated, not to help community members, but simply for the sole benefit of the data collector.

I don't trust data-driven systems, though data could be used for better. Our interviewees expressed a distrust of data systems, though acknowledged that data could be used in positive ways and made suggestions towards that end.

I believe in privacy, but I don't think there's much I can do to protect it. People desire and care about privacy, but feel like they have no choice but to give up information.

Data is a power relationship. Data collection often diminishes the agency and limits the self-determination of targeted individuals and communities.

Data systems write me off for being poor. Our interviewees find that data-driven systems—and sometimes the people behind them—treat them poorly for being poor.

Innovation, resistance, and self-defense. Despite feeling tracked and trapped by data collection, interviewees have shared innovative strategies for survival and data self- defense.

ACTIVITY: Get 'Em Thinking About Data

Time: 45-90 minutes **Group size:** 5-45

OVERVIEW

This activity is the activity to start with, the quick-and-dirty version of all of our Playbook sections and parts. During this workshop, participants will gain a deeper understanding of data, what it is, and how it impacts our lives; explore "what's in their wallets" with a hands on activity that describes data collection and its impacts; and, develop community-based self-defense tools that will leave them feeling inspired and ready to dig deep into the power they possess.

GOALS:

- Provide a basic introduction to data, data collection, and data systems
- Explore how data and data collection are apparent and affect our lives daily
- Begin developing community defense tools

SUPPLIES:

Butcher paper, marker, sticky notes, ODB quotes, tape

PREPARE BEFORE THIS SESSION:

Prepare the quotes from the *ODB Quote Bank* (see pp.22-24), review sections for deeper explanation if needed.

CONTENT

OPENING (20-30 MINS)

INTRODUCTIONS (5-10 MINS) Go around the room, and have each person introduce themselves, providing their name, gender pronoun, and community/ organization they represent.

STORY SHARE (10-20 MINS) In small groups have the participants answer the following question: "What data systems did you have to engage with to get here today and what information did you provide to those systems?"

Provide an example to help the room generate their own ideas, such as:

- "I used Google maps and it collected my location."
- "I used my debit card to buy breakfast and that used my location, what store I shopped at, and what I ate."
- "I logged into my Facebook account and checked in at my favorite restaurant sharing my location and personal likes or a place I visit often."

REPORT BACK (5-10 MINS) Ask the room to share some of the systems they engaged with and the data that was collected. Take notes on large paper. You can pose to them the following questions:

- "Thinking about what information was collected, how do you feel?"
- "Had you considered what information you were exchanging before you got to this workshop?"
- "What has changed hearing others stories?"

OUR DATA, OUR STORIES (20-30 MINS)

READING QUOTES (10-15 MINS):

(1-2 MINS) If participants are not already in groups, have them break up into small groups for this section. (Each group should have 2-5 quotes and a blank piece of paper.)

(5-10 MINS) Invite each group to read each quote out loud to each other.

Depending on the size of the group you can either:

- Post the quotes around the room and have the small groups do a gallery walk to read and interact with the quotes and choose one to bring back to the larger group, or
- Have the 2-5 quotes already at each working group table for them to engage with.

GROUP DISCUSSION (10-20 MINS):

(10-15 MINS) After the group has read the quotes to each other, ask them to answer the following question: "After hearing the experiences that brought us into the room during our story sharing and the quotes you have just read, think about what theme(s) are coming up? Discuss them and write all of the themes on the blank paper at your table." Be sure to prompt the groups to write their themes on the blank paper half way through the time.

(5 MINS) Ask the group to report back to the room. Popcorn style, go around the room asking individuals to uplift some of the themes they noticed. Ask folks for general reflections and thoughts about what's coming up.

FLIP THE SCRIPT (10-20 MINS)

In this section, participants will begin developing/generating solutions for the themes they have identified.

(5 MINS) Instruct the small groups to collectively pick one theme (or a combination of some of the themes) to work with. After 5 minutes, check in with folks to make sure they have their theme(s) and are ready to move on.

(10 MINS) After selecting a theme have the group:

- Literally flip over the paper with the themes on them
- Write their collectively chosen theme at the top of the paper
- Collectively generate some solutions/tactics to address the theme they chose
- Be prepared to share one or two solutions with the large group

(5 MINS) After the whole room has gone, have each group hang their solutions around the room. Take in the solutions and the collective power they have generated.

CLOSING (5-10 MINS)

It is important for participants to have a sense of closure and transition at the end of a session. Invite participants to choose from one or more of the following prompts:

- Share one word that represents how they are feeling right now (i.e. powerful, confused, supported, challenged, etc.);
- Use their body to express how they are feeling right now;
- Share one thing they are taking with them from the workshop;
- Share something they learned that they want to share with someone else;
- Share something about their community that they are grateful for; or
- Share a question that came up for them.

Document all the questions. Some questions can be answered in following or future sessions. Questions are a great way to generate more community-based research.

ACTIVITY: Whatchu' Know about Data?

Time: 45-90 minutes **Group size:** 5-25

OVERVIEW

This activity is designed to help participants gain a deeper understanding of the term "data," what it actually means and represents, and the different types of data that exist.

GOALS:

- Provide a basic understanding of data, what it is, and how it impacts our lives
- Develop a collective community definition of data
- Identify what types of data we encounter every day

PREPARE BEFORE THIS SESSION:

Review the *Whatchu' Know About Data?* PowerPoint (https://bit.ly/2STD9qm) and make notes of the different types of data you want to explore or address during this workshop; write a formal definition of data on big paper. See definition provided in *Commonly Used Terminology. (*p.19).

SUPPLIES:

Butcher paper and markers (for group note taking), strips of paper, pens, markers

CONTENT

OPENING (20-30 MINS)

Say, "Everyday, more and more, on the news, TV, phone, or internet, we frequently hear the term 'data' being used. There's 'unlimited data,' 'data overages,' 'data plans,' 'personal data.' But who actually knows what they are talking about? Today we will be exploring the concept of 'data.'"

INTRODUCTIONS (5-10 MINS): Name, gender pronoun, community/organization they represent.

STORY SHARE (10-20 MINS): In pairs have the participants answer this question: "When you think about or hear the term data, what comes to mind?"

Guided Questions:

- "What images do you see?"
- "What experiences does it make you think about?"
- "What are some ways "data" shows up in your life?"

REPORT BACK (5-10 MINS) Ask each pair to report back one or two things that came up during their conversations. Chart what they have come up with on large paper for the group to review.

DEFINING DATA (10-20 MINS)

This section will take a deeper dive into developing a collective understanding and definition of data and the different forms it takes.

Prompt: "Data can be many different things. It can be digital, personal, interpersonal (person to person). It can be collected by us or from us, provided to us by companies, or taken from us by companies. Data can be used to make decisions about us, to craft or tell our stories, or even connect us to something, someone, a service or to be criminalized. Data and how we use or understand it is vast, as we can see from the list we generated."

Facilitators note: refer back to group list and point out some of the main categories that stick out or that are similar. Some examples of data include social media posts, our browsing history on the internet, ads we click on, our DNA, job applications, e-mail address, records, rental history, income level, how many children we have, driver's license number and past history, school records, EBT food stamp purchases, evictions, grades, etc.

DEFINING DATA COLLECTIVELY (10 MINS)

In this section participants will work together to develop a collective understanding of data and gain a deeper understanding of how it translates into our lives.

1. In the large group, review the formal definition of data: "Data is: facts, details, statistics, or any information collected together for reference or analysis." Write on big paper or show via PowerPoint.

2. In the large group, brainstorm ideas to help build a new collective definition of data

   Prompt: "If we had to build or develop our own definition of data what would you add?"

Facilitators note: popcorn style in the large group, write the suggestions down on the same paper/presentation the formal definition is written on and have a blank paper to write down the final new collective definition.

3. Review new definition with the large group by synthesizing what you've heard, ask for a collective vote to accept the definition.

DATA IS NOT (15 MINS)

In this section participants will gain a deeper understanding of how all data is not created equal.

Prompt: "Now that we have defined what data is, it's important to know what data is not." Compare with the definition of data (see "Commonly Used Terms," p.19).

Data is not all digital: "Not all data that is collected is in the digital form. Just like we noted earlier, data can take many forms including: gossip, DNA, conversations we have, and our past history."

Not all data is equal: In pairs or small groups have participants generate some types of data that may not be created equally.

Prompt: "Some of the data that is collected or generated about us isn't there to help us or to determine if we are capable of doing something. Sometimes its sole purpose is to be used to block us out of an opportunity or to classify us in ways that impact our lives and our ability to provide for ourselves."

Guided Question (small group or pairs): "Think about a time that you, your friend, or family member were possibly denied for a job, school, an opportunity. Consider what type of data—or information—was collected to make that decision and what was the outcome of them being denied."

Large group report-back: In a popcorn style, collect 3-5 types of data that isn't created equally and an outcome of them being denied or hindered.

CLOSING (5-10 MINS)

Prompt: "Now that we have a collective definition of data, a better understanding of what data is, and how it impacts our lives, ask yourself:

- How will knowing this information help you navigate the data world? And how you engage with it?
- Do you currently use any tools to keep your digital and person data safe?"

ACTIVITY: Let's Create A Data Stream

Time: 30 minutes **Group Size:** 5-25

OVERVIEW

Participants will create a data stream to experience how people's identities are made when random pieces of data are collected and linked together.

GOAL:

- Illustrate how our different points of data can construct a narrative about who we are, which may be used in decision making

PREPARE BEFORE THE SESSION:

Prepare paper strips.

SUPPLIES:

Sheets of paper cut into strips, pens, markers, tapes, timer

CONTENT

OPENING (15 MINS)

INTRODUCTIONS (5 MINS): Name, gender pronoun, community/organization they represent.

STORY SHARING (5 MINS): In pairs, have participants answer the following question: What information, if any, do you feel follows you around, so much so that you can't shake it off? How does it make you feel?

OPEN DISCUSSION (5 MINS): Introduce the meaning of a data stream. From the "Commonly Used Terms"(p.19) section, data stream is defined as: "The sharing of a persons collected infromation from institution to institution; how systems talk to each other." Prompt: How do the stories you shared connect to this definition?

LET'S CREATE A DATA STREAM (5 MINS)

- **Step 1:** Hand each participant a piece of paper (usually no larger than ¼ or ½ of sheet).
- **Step 2:** Each person will have 10 seconds to write down a random word. Note that you will cue when time starts and begins.
- **Step 3:** When the 10 seconds are up, everyone should switch papers with someone else in the group.
- **Step 4:** Repeat steps 2 and 3 for four total rounds
- **Step 5:** After the fourth swap, the person is to use all four words on the paper to construct a sentence.

Have some participants volunteer to read the sentences out loud to the groups.

REPORT BACK/GUIDED QUESTIONS (5-10 MINS)

- How was this exercise like a data stream?
- How does this apply to us and our lives?
- How can you use this knowledge?

CLOSING (5 MINS)

Suggest to participants that the bits and pieces about ourselves that we share in different places or spaces are used to tell stories about ourselves. Have participants reflect on the question: What is the story that you want data to tell about you?

ACTIVITY: I Can See Your Data Trail!

Time: 45-90 minutes **Group Size:** 5-25

OVERVIEW

In today's society social media and other media profiles have become an interwoven aspect of our everyday lives, whether it is sharing photos on Facebook or having an Indeed job search profile. These sites keep data about us that can be used to inform decision that have a serious impact on our lives.

In this workshop participants will explore our data trail, how private and public facing we are, and how to protect ourselves and our digital information.

GOALS:

- A deeper understanding of private versus public information and how their data can be accessed
- Gain a deeper understanding of how data trails may impact our lives
- Learn more about privacy settings and features on our social media accounts

SUPPLIES:

Computer or smart phone, pen, paper, *I Can See Your Data Trail* Worksheet (p.37)

PREPARE BEFORE THE SESSION:

View our tips on data security and privacy to become familiar with how an individual's information is collected and shared in order to make decisions and how to make social media accounts private.

CONTENT

OPENING (30-40 MINS)

Today we will dig into what personal versions of ourselves is available for the public to see and make decisions about ourselves.

INTRODUCTIONS (5-10 MINS): Go around the room and have each person introduce themselves providing their name, gender pronoun, community/organization they represent.

STORY SHARING (10-20 MINS): In pairs or small groups answer the following question. “From a scale of 1 to 10 [1 being the not private or very visible at all and 10 being 100% private or not at all visible] how would you rate your web visibility?

REPORT BACK (5-10 MINS): Popcorn around the room to hear from the participants how visible they think they are. Be sure to ask them why!

PARTNER PROFILES (20-30 MINS)

In this section, participants will dive into understanding how and who we are on the web, and if it actually represents who we are in our everyday lives.

1. Break participants up into pairs. Once in pairs, have participants introduce themselves to each other. Name, gender pronoun, community/organization they represent.
2. Each participant should receive a partner questionnaire (see worksheet below). Partner A should interview Partner B and answer only “Part A” of the questionnaire. Once complete partners should switch.
3. Once the partner questionnaires are complete, have each partner take 10-15 minutes to use the information provided to conduct their own research. Use Google, Google images, or any information they provided to see what folks can dig up.

Once the time has elapsed, have the partners compete “Part B” of the questionnaire.

Debrief: Have each pair talk about what they found about one another. They should review the questioners with each other and answer the following:

- What things did you find on your partner?
- What profiles were visible?
- What images did you see?

Go over the answers to Part C with each other.

CLOSING (5-10 MINS)

Ask participants the following questions: "Was what your partner found out about you accurate?" "Did it align with the privacy score you gave yourself at the beginning of the workshop?" "What did you learn about your virtual self? and "What will you do differently moving forward?"

Point participants to digital security resources in "Our Community Bag-of-Tricks" (p.90).

WORKSHEET: I Can See Your Data Trail

	Partner A Questionnaire	Partner B Questionnaire
PART A	Partner B Name	Partner A Name
	Partner B Birth Date	Partner A Birth Date
	City, State, Zip Code	City, State, Zip Code
	Social media profiles	Social media profiles
	Facebook	Facebook
	Instagram	Instagram
	SnapChat	SnapChat
	Other	Other
PART B	Using the info partner B provided, search the web to see what you can find. Did you find info about your partner?	Using the info partner A provided, search the web to see what you can find. Did you find info about your partner?
	❑ Facebook Profile (private/not private) ❑ Instagram profile (private/not private) ❑ Photos ❑ Family/Friends ❑ Work Place/Job ❑ Personal Past History ❑ Other: _____	❑ Facebook Profile (private/not private) ❑ Instagram profile (private/not private) ❑ Photos ❑ Family/Friends ❑ Work Place/Job ❑ Personal Past History ❑ Other: _____
PART C	Based on the info you found on Partner B, create a description of this person. Be sure to include the info you found, assumptions you may have, and general observations you witnessed. _____ _____	Based on the info you found on Partner A, create a description of this person. Be sure to include the info you found, assumptions you may have, and general observations you witnessed. _____ _____
	In your opinion, is it easy to find info on this person? Yes / No? Based on what you’ve seen, if you had to hire this person, would you? Yes / No? Why? _____	In your opinion, is it easy to find info on this person? Yes / No Based on what you’ve seen, if you had to hire this person, would you? Yes / No? Why? _____

DATA BODY CHECK-UPS

ACTIVITY: Your Data Body

Time: 45-60 minutes **Group Size:** 5-25

OVERVIEW

Although virtual, digital data collection and surveillance can physically impact us as humans and weigh us down. From time-to-time, we need to take a step back to identify the shape we are forced to take and re-shape ourselves towards resilience.

Participants will explore their digital bodies, including their shapes, and create a model of resilience.

GOALS:

- Explore how and what data impacts our physical bodies
- Identify the shape of our data body
- Create a new one

SUPPLIES:

Blank paper, pens, *Your Data Body* Worksheet

PREPARE BEFORE THE SESSION:

On a large sheet of paper, draw an outline of a body.

CONTENT

OPENING (15 MINS)

"Today we will dig into what our data bodies actually look like and start to think of ways we can make a new shape under the current system."

INTRODUCTIONS (5-10 MINS): Go around the room and have each person introduce themselves, providing their name, gender pronoun, community/organization they represent.

STORY SHARING (5-10MINS): "Take a moment and draw a logo that represents who you are and share it with a partner."

REPORT BACK (5 MINS): Popcorn around the room to hear from the participants, have them showcase what they drew.

UNDERSTANDING OUR DATA BODIES (15 MINS)

In this section, participants will dive deep into what a data body is and explore the different aspects that compose it.

OPEN DISCUSSION (5 MINS): In a large group, small groups, or pairs ask participants to answer the following question: "When you hear the term 'data body' what comes to mind? What visuals do you see? What other words or terms do you associate with it?"

REPORT BACK (10 MINS): Popcorn style or go around the room collecting answers from the group. Write the answers on large butcher paper.

Explain that most times our data bodies live in the digital world. However, our data bodies do have an impact on our physical bodies, because they are used to make decision about us, our lives, our families, and our ability to meet our basic human needs. There are three main aspects of a data body: the data itself, the institutions that collect or control it, and the needs and support our bodies must have met or receive.

OUR COLLECTIVE DATA BODY (10 MINS)

Say, "In order to further understand what our data bodies actually are, we are going to create one large data body collectively."

Data Body Prompt: "What are some aspects/types of data that are collected about you? What types of data live within your data body?" Use the body outline to take notes. Add the types inside of the body.

Data Body Control Prompt: "What types of data systems/social service organizations/ other organizations use or collect this information about us?" On the same paper, add the types of institutions outside of body.

Data Body Support/Needs Prompt: "What things/services/needs are you trying to meet or receive when this information is collected about you?" "On the same paper, add the types of needs to the bottom of the body, under the feet.

In pairs, have participants discuss some general reflections and observations about the collective data body. Ask them to also discuss the ways they protect their data body. Popcorn some thoughts and draw a circle to represent continued protection around the body and write some the protection tactic.

MY DATA BODY (10 MINS)

Say, "Now that we have designed a group Data Body, we are going to take a look into our personal data bodies."

UNDER SURVEILLANCE (5 MINS): Hand out worksheets. Have participants draw their data bodies under data collection and digital surveillance (the left box of the worksheet). In pairs have them talk about what they drew.

FREE FROM SURVEILLANCE (5 MINS): Have participants finish the other box on the worksheet drawing what their bodies look like when they are free from data collection and digital surveillance. In pairs, have them talk about what they drew.

Give participants time to answer the questions at the bottom of the sheet, ask for a few volunteers to talk about what they drew and to answer the questions out loud.

CLOSING (5 MINS)

Say, "When thinking about our data bodies and the shape they currently are and what shape we want them to take in the future, it is important for us to remember that we have the tools and skills to protect ourselves and each other. So we will model what our bodies look like free from data collection and digital surveillance."

- Ask participants if they are willing and able to stand. If they are not willing or able, it's ok, this exercise can be done seated.
- Ask participants to move their bodies to mimic the drawing they created of their bodies under data collection and digital surveillance. Have them look around the room.
- Ask participants to move their bodies to mimic the drawing they created of their bodies free from data collection and digital surveillance. Have them look around the room. Remind them that freedom is possible and refer back to the tools around the group's data body for tools they currently have to help them reach this state.

Optional closing: Share the ODB definition of a data body, which points to control, needs, and institutions. "Discrete parts of our whole selves that are collected, stored in databases, the cloud, and other spaces of digitally networked flows, and used to make decisions or determinations about us. They are a manifestation of our relationships with our communities and institutions, including institutions of privilege, oppression, and domination."

WORKSHEET: Your Data Body

Please fold this paper along the dotted line and follow the instructions for each box.

Draw a picture of your data body under the surveillance state.

Draw a picture of your data body after the surveillance state has been dismantled.

Please answer the following questions:

1. What is the same between your two data bodies?

2. What is the difference between your two data bodies?

3. What needs to change to help you free your data body?

ACTIVITY: What's in Your Wallet?

Time: 45-90 minutes **Group Size:** 5-25

OVERVIEW

This activity opens up participants' awareness of the different kinds of data collected by institutions that we rely on every day and equips participants with popular education tools to begin developing their digital defenses. This activity pairs nicely with the Draw Your Data Body activity.

By the end of What's in Your Wallet, participants should feel more confident in talking about the basic kinds of data that institutions collect in their day-to-day lives and be ready to think about what might be right, wrong, good, and bad about these data and the processes of collecting them.

GOALS:

- Build knowledge about digital data collection using a physical object that most people carry around with them
- Cultivate an awareness in order to start defending ourselves against harmful data collection and to support da-ta-driven processes we find beneficial

SUPPLIES:

What's In Your Wallet Worksheet (p.46), pens

PREPARE BEFORE THE SESSION:

Think about arranging the seating in the room so that it is easy to work in pairs.

CONTENT

OPENING (20 MINS)

"Welcome everyone. We're going to spend a little time thinking about: What makes up your data body (online identity)? And we're going to do that with a hands-on activity that gets us thinking about everyday data collection and reflecting on the different kinds of data we depend on to get by in life."

INTRODUCTIONS (5-10 MINS): You can run a seven-minute "smeeting" (speed meeting) in which you pose a question, then ask people to find someone they don't know and answer that question. Each exchange should last no more than a minute, and participants can popcorn what their partners shared for one minute each. Ask:

- "What is one cool thing you've experienced today?"
- "What comes to mind when you think about data?"
- "What more do you want to know about data?"

REPORT BACK (5 MINS): Popcorn around the room to hear from the participants. Have them showcase what they heard or shared.

FINDING THE DATA OF OUR EVERYDAY ACTIONS (15 MINS)

Hand out and walk participants through the worksheet.

DIGGING THROUGH YOUR WALLET (5-10 MINS): To get people started, you can say: "We're going to ask you to take out your wallets to complete this exercise. Here's a worksheet that asks you to catalog any kind of card you have in your wallet and the kinds of information that is recorded on that card or that you had to give up in order to use that card, benefit from some service that card provides, or engage in some sort of transaction that the card lets you do. Take out all the cards, write the cards on the worksheet, and draw a line to the type or types of data they rely on to work. Note: if you don't see your data listed, write it in, and then draw a line connecting your card to that type of information."

PROMPT (5 MINS): Invite people to discuss the following questions in a large group:

- "According to your worksheet, which kinds of data gets collected the most? What are, for example, the top three kinds of data that gets collected?"
- "Do you see any patterns in data collection across the different cards you use?"
- "What kinds of data do people have on their worksheets?"
- Have people popcorn as many as is possible. Where possible, probe for differences and similarities.
- What does this activity make you think about with respect to data collection?
- What questions or concerns come to mind when doing this activity?

FOLLOW-UP (5 MINS): Ask:

- "Is there any card that collected information from you that you were happy to give up? Or that collected information in a way that you were ok with?"
- "How does data collection connect to your neighborhood? To a community or group you belong to?"

CLOSING (10 MINS)

Introduce the definition of a data body that ODB uses. Say: "Our data bodies are discrete parts of our whole selves that are collected, stored in databases, the cloud, and other spaces of digitally networked flows, and used to make decisions or determinations about us. They are a manifestation of our relationships with our communities and institutions, including institutions of privilege, oppression, and domination."

Invite participants to reflect on this definition, including how it resonates with them now that they have completed the What's in Your Wallet activity. Ask: "Now that you've had this experience, what more do you want to learn about data and/or data collection?"

Follow-up with: "What are you doing to protect yourself? What are some ways we can think of to keep ourselves, our communities, or our data safe?"

WORKSHEET: What's in Your Wallet?

1. What makes up your online identity?

First, draw the cards in your wallet in the workspace below. Then, draw lines between each card and the types of information that were collected to receive the service.

Card Type	**Social Security number**	*Card Type*
	Address	
	Phone number	
	Birthdate	
Card Type	**Work information**	*Card Type*
	School information	
	Health information (eye color, weight, height, etc.)	
Card Type	**Marital status**	*Card Type*
	Emergency contact/ references	

2. What does this activity make you think about with respect to data collection?

3. What questions come to mind when you think about data collection and your "data body" (e.g., online identity)?

4. How does your data body connect to your neighborhood/community?

ACTIVITY: Are You Sharing? I Might Be.

Time: 45-90 minutes **Group Size:** 5-25

OVERVIEW

In this activity, we dive into what it means to share data, including in situations where we want to share and those in which we do not.

GOALS:

- Gain a deeper understanding of how information about ourselves is shared, how we intentionally and unintentionally share our information
- Develop some tools or steps we can take to keep our information safe

PREPARE BEFORE THE SESSION:

It is a good idea to read the *Community Defense Toolkit* (p.81), in this Playbook. The sections *Credit Score, Credit Report: What's It Got to Do with Me?* (p.85) and *Data Brokers and Opting Out* (p.88) can provide useful background.

SUPPLIES:

Are You Sharing? I Might Be (p.51) Worksheet, pens, markers, paper, smartphones/laptops, access to the internet

CONTENT

OPENING (30 MINS)

Say to participants, "Welcome everyone. This session is about understanding how we share information about ourselves, as well as how others share information about us. The ways in which data are shared shape how institutions and people define us, understand us, judge us, and treat us."

INTRODUCTIONS (5-10 MINS): Go around the room and have each person introduce themselves, providing their name, gender pronoun, and community/ organization they represent.

STORY SHARING (10-20 MINS)

Ask participants to break out into small groups or pairs. Instruct them to ask each other: "Do you read the security and privacy statement when you are downloading new apps/ applications on your phone, entering a new website, or entering data into a system and it askes you to agree? Why or why not?"

REPORT BACK (5-10 MINS): Popcorn around the room to hear from the participants, take note of the whys and why nots.

DATA SHARING (10-15 MINS)

Say, "In today's day–and-age, there are two primary ways we as consumers share data or information about ourselves: intentionally and unintentionally. Intentional data sharing is when we know we are sharing information about ourselves, whether we want to or not; like when we fill out job applications, post on Instagram, or share our location using Google."

Ask the group to give more examples of how, when, and why they intentionally shared data about themselves.

Continue by saying, "Unintentional data sharing is when we don't know data is being collected about us, for example we may use applications on our phone that share what Facebook post we like, or using food stamps (SNAP benefits) may share what kind of food we buy with our caseworkers."

Go back to the question about clicking the data "accept terms and conditions" question. Use this as an example of unintentional sharing. Ask some participants to share when and what was the last time they clicked yes.

You can explain, "Just because you intentionally gave your information away, doesn't always mean it was 100% voluntary or that you wanted to comply and sometimes the intentional and unintentional data sharing are connected."

Say, "For example, when we fill out a job application we give them permission to go into our backgrounds, give them our educational history, and permission contact our references. But we don't really want them calling our folks or reading our past to make decisions about our future."

Ask and record on large butcher paper: "What are some data we intentionally give up, but may not want to?"

INTENTIONAL DATA WATCH (15-20 MINS)

This section will help participants gain a better/deeper understanding of the intentional types of data they are sharing.

In pairs, have participants exchange one social media profile of theirs. If they are not on social media, their full name or the name of a close friend or family member.

Instruct the partner to look through the first 5-10 posts of their partners to see if they can find any of the following information about them:

- A place they have visited (name and location)
- The name of a family member or friend
- Where they work or live
- A favorite spot to visit

After they are done, have the pairs report back what they found on each other and answer the following questions:

1. Did you intend on sharing that information? Was it shared on purpose? Did you know you shared that?
2. How does it make you feel knowing someone can gather that information about you just by glancing at your social media?
3. How much intentionally versus unintentionally shared information did your partner find?

DIGGING DEEPER (15-20 MINS)

In this section you'll introduce the Worksheet. Say: "Social media is just one of the platforms, we use to share information about us. Many other companies collect information about us."

Ask the group to name some other types of places/ locations/ services where their information is shared both intentionally and unintentionally. Take notes on large butcher paper.

Hand out the worksheet.

Using what they just heard, the activity with their partners, and their knowledge on how they share information, ask participants to complete the worksheet. Say: "Think of 5 different types of data you share about yourself, using what we learned/discussed today and other experiences. Note whether or not it was intentional or unintentional data sharing and explain how it is collected."

Then instruct them further, "In the boxes below, chart the types of data into the boxes on how you share them." You can tell them it is ok to use one dataset more than once.

CLOSING (5-10 MINS)

After everyone has completed their worksheet, break up into pairs and have them discuss what they found answering the following questions:

- "Are there any overlapping items on your chart? What are they and where do they land?"
- "Looking at the charts, what types of data will you share differently, more of, or less of?"
- "What types of data do you think should be collected about you that isn't? Or which types shouldn't be collected about you at all?"

Again, draw participants' attention to the resources in the *Community Defense Toolkit*. (p. 81) Point them not only to the different info sheets, which provide some guidance about opting out of data collection, correcting wrong information in databases, etc., but also the *Community Bag-of-Tricks* (p.90).

WORKSHEET: Are You Sharing? I Might Be.

Data is shared in two different types of ways, Intentionally and Unintentionally:

Intentional Data Sharing: *is when we know we are sharing information about ourselves, whether we want to or not; like when we fill out job applications, posting on Instagram, sharing your location using Google.*

Unintentional Data Sharing: *is when we don't know data is being collected about us, for example we may use applications on our phone that share what Facebook post we like, or using food stamps (SNAP benefits) may share what kind of food we buy.*

What data are sharing?	Are your sharing it intentionally or unintentionally	How are you sharing it?
Example: My Picture	❑ Intentionally ❑ Unintentionally	Example: Facebook, Instagram, SnapChat
	❑ Intentionally ❑ Unintentionally	
	❑ Intentionally ❑ Unintentionally	
	❑ Intentionally ❑ Unintentionally	
	❑ Intentionally ❑ Unintentionally	
	❑ Intentionally ❑ Unintentionally	
	❑ Intentionally ❑ Unintentionally	

In the boxes blow, write down the types of data you love sharing, want to share, don't want to share, and have no choice but to share.

I love sharing this data	I want to share this data
I don't want to share this type of data	**I have no choice but to share this data**

1. Are there any overlapping items on your chart above, if so, what are they?

2. Look at the charts above, what types of data you share, will you share your data differently?

3. What types of data do you think should be collected about you that isn't? or which types shouldn't be collected about you at all?

ACTIVITY: My Data Check-Up

Time: 45-90 minutes **Group Size:** 5-25

OVERVIEW

In this workshop, participants map their social networks to see how and whether people or institutions in these networks are sharing information with each other. By the end of this workshop, participants should have a greater awareness of what they and their networks are already doing to encourage safe data sharing and what they might consider doing differently.

GOALS:

- Recognize the variety of tools we use for communicating or sharing data, including those that we create and manage, versus those that others make available and sell to us
- Reflect on what's appropriate, acceptable, or consensual when sharing information

SUPPLIES:

Markers; Pink, yellow and orange post-its, including skinny and large ones; Butcher/flipchart paper (or a surface you can stick post-its onto and draw on); six large post-its or papers that you can tape up (that say, "Voluntary," "Involuntary," "Control," "Lack of Control," "Me," "My Whole Social Network"); 11 x 14 sheets of paper; *My Data Check-Up* Worksheet (p.58)

PREPARE BEFORE THE SESSION:

Make sure that you have two big sections of wall space. The right side will be devoted to people mapping their social networks and tools. The left side will be devoted to people mapping their protective tools, services, or practices.

CONTENT

OPENING (30 MINS)

Say, "We're going to spend the next hour mapping our social networks, the kinds of communication we use when we interact with people, groups, organizations, and institutions. These might be our friends, family, people who we don't know very well, places whose services we use a lot, or places we use only a little bit. Our goal is to get a sense of all of the different services, tools, or practices we use to communicate and share data about ourselves, and to consider how much control we have over them."

INTRODUCTIONS (10 MINS): Go around the room and have each person introduce themselves providing their name, gender pronoun, community/organization they represent.

STORY SHARING (10-20 MINS)

Say, "Individually, think of your social network: the people, groups, organizations, and institutions, etc. that you deal with on a routine basis. Jot down who is represented in your network."

REPORT BACK (5-7 MINS): Ask the room to share some of the items they listened within their social network. Take notes on large paper.

MY DATA CHECK-UP (20-30 MINS)

This section consists of five steps.

1. Using the 11 x 14 paper, have participants draw an image, icon, word, or logo that represents them.
2. Referring them back to the earlier prompt, give them the hand out to help guide them through the next process. ("We will be using this document for the rest of the workshop"). Make sure to:

    - Have participants transfer their list to Side A of the worksheet and fill out the sections.
    - Prompt participants to ensure they are moving along. Encourage groups or pairs to talk to each other.
    - Ask for the group to give you examples after each section and jot them down, so you can develop the larger network while participants are working.

Facilitator's note: For the next section, it may be useful for you to have you own larger version using the large butcher paper so folks can be clear on the instruction and have a visual to help guide them and to also have tape and extra 11 x 14 papers on the desk in case folks need more space to work with.

3. Using the small pink post-its, instruct participants to write/transfer the "who's in my network" list to their large paper using the pink post-it notes. Remind them to only use one post-it per person, group, organization, or institution to visualize their social network.

Facilitator's note: While the room is mapping their individual networks down, you should map the ones the group came up with collectively. This will be the large group representation.

Have participants report back. Give them 2-3 minutes to showcase what they have down and what their networks are beginning to look like.

4. Using the small yellow post-its, instruct participants to write down methods and mechanisms they use to communicate—or their "communication strategies." This can include plain-old voice and new types of digital technologies, such as a website forms, mobile phone, or chat apps. Have them write one communication method/ mechanism per post-it.

Say, "Some communication strategies, like Gmail post-its, will repeat if that's a means by which you communicate or share information about yourself with different people, groups, organizations, or institutions. It's ok!"

When you're done mapping the large group representation, instruct participants to cluster/place the yellow post-its around the person, group, organization, or institution it corresponds to. While participants are writing, ask them to shout out some of their communication methods and to whom so you can map it for the group.

5. Once completed, have participants hang their networks on the same wall and invite folks to do a gallery walk.

REPORT BACK (15 MINS): Ask participants:

- "Looking at our large network and everyone else's, what are some things that are coming up?"
- "Is there anything that needs to be added to our collective mapping?"

Invite folks to actually come up and add to the collective mapping, and spend some time on general reflection.

CHECKING OUR COLLECTIVE NETWORK (20 MINS)

SPECTRUM MAPPING (10 MINS): For this portion participants will explore how they engage with the sharing of their information based on the thematic or group clusters that you, the facilitator, has helped surface in the large group map you've been drawing. For each prompt pick 2 to 4 clusters to go through. Examples of clusters for "my networks" might be: family, social worker, doctors, parole officer, pastor, where I work, etc. Examples of clusters for "communication strategies" might be: referrals, calling on my mobile phone, Gmail, in-person communication, web form, etc.

Say: "As a group, we will identify where our post-it clusters belong by aligning ourselves along a continuum. For each turn, I will announce to you the ends of the spectrum. Using you own personal experience, move to the location on the spectrum based on what you believe. I will ask for volunteers to explain why they are standing where they

are." You can remind participants that shifting around is ok! Do a test run with the following example: I love eating vanilla ice-cream. On one side of the spectrum is "I love it" and on the other side is "I hate it." Have folks move to where they are on the spectrum. Answer any questions.

VOLUNTARY/INVOLUNTARY: "When I share information with or by [insert cluster title], I voluntarily provide the information." Instruct people to move towards involuntary if they do not provide that information themselves—that is, if they are forced to provide it. Say, "Move to or towards voluntary if you are willing to provide the information, that is, if you decide to share it."

CONTROL/LACK OF CONTROL: Repeat the spectrum activity with the next prompt: "When sharing my information with [insert cluster title], I take my information back. Stand by 'control' if you can take it back. Stand closer to 'lack of control' if you cannot."

REPORT BACK (10 MINS): Once seated have participants answer:

- "What were some things that stood out? What was different? What was surprising?"
- "How do you feel about how you are sharing information, what you can and cannot control, etc.?"

POWER NOT PARANOIA (10-15 MINS)

Say, "In this last part of the activity, we're going to generate/develop/identify the ways we protect our information."

Have each group pick a cluster from the large group mapping to work on.

Instruct each group to have one note taker. Have them generate ideas on the ways, tools, services, or practices they can use to protect or control the ways in which they share information.

Have them transcribe it to the orange sticky notes, and when they have finished have them post it to the large group map.

REPORT BACK (5-10 MINS):

Uplift the cluster name and some of the ways we can protect yourself.

Ask, "Thinking about the activity, the spectrum network, and now the orange post-it-notes and the solutions we generated, how do you feel? What has changed?"

CLOSING (10 MINS)

Pose the following questions to participants:

- "In the time remaining, we have a little bit of time to ask the following questions:
- "What different factors impact how you communicate and how much you protect your communications?"
- "What are your thoughts on increasing protection in our networks, in our communities?"
- "How useful is this exercise for the communities you work in, live in, and care about? What works, and what doesn't? How would you change this activity?"

WORKSHEET: My Data Check-Up

Please complete the following:

Side A: My Network Is....	Side B: I communicate with them by...
Ex. Doctors and Hospitals	Calling, appointments, referrals

Please identify a theme (aka cluster title) that helps you categorize any of the information you listed above.

What tools, services, or practices can you use to protect the information that you share?

ACTIVITY: Mapping Your Data Self

OVERVIEW

In this activity, participants will map their electronic selves and who has access to their information.

GOALS:

- Gain a deeper undersigning of what information is being collected, stored, and shared about us
- Develop and identify tools to help keep our, and our community's, information safe

SUPPLIES:

Mapping Your Data Self Worksheet (p.62), paper, pin, markers, butcher paper, tip sheet for keeping our data safe

PREPARE BEFORE THE SESSION:

Please read the *Community Defense Toolkit* (p.81), especially the sections focused on data brokers and credit scores.

CONTENT

OPENING (20-40 MINS)

Say: "We're here to explore who has access to data—electronic information—about you, how they store and search it, and who they share it with."

INTRODUCTIONS (5-10 MINS): Go around the room and have each person introduce themselves providing their name, gender pronoun, community/organization they represent.

STORY SHARING (10-20 MINS)

Take a moment, look through one of your social media profiles and find an image that would represent your digital brand. Share with a partner the photo, brand name, and why.

REPORT BACK (5-10 MINS): Popcorn around the room to hear from the participants.

MAPPING OUR DATA SELVES (30-40 MINS)

Give everyone a handout and pen.

Instruct participants to complete part A of the worksheet by writing down or drawing all the different kinds of electronic information that is collected about them (inside of the body shape). Be sure to give an example of a type of data to start them off. For example, school collected my previous education history. Jobs collect my social security number, etc. Also, reassure them that there is no right or wrong answer.

After they have completed the task, have participants draw lines from the images surrounding the data body if that item, service, entity, etc. collects two or more different data points from them.

After that, have participants draw lines from the entities that may share information about each other. Example, a school might collect your license plate info for parking.

PAIRED DISCUSSION (10 MINS): In small groups or pairs have the participants share their handouts with each other and talk about their findings. Ask them to answer the following questions:

- "What data is being collected the most?"
- "What data is being collected the least?"
- "How much of your data body is being accessed for services?"
- "What are the primary ways this information is being collected?"
- "How does it make you feel to know this?"
- "Does anything change?"

REPORT BACK (10 MINS): Popcorn around the room to hear from the participants and write the answers to the questions on big paper. Identify what themes are coming up.

DIGGING DEEPER (10 MINS): Still working in pairs or small groups, have participants pick three different points of their digital data and complete the chart at the bottom of the worksheet. Have them discuss what they find, including

- "Who collects this data?"
- "Where is it stored?"
- "Who is it shared with?"
- "What rules apply to its collection, use, sharing?"

Ask them what information they are noticing that they don't know. Be sure to capture this on large, butcher paper.

Ask, "What rules do you think should exist to cover electronic information collection, sharing, storing?"

REPORT BACK (10 MINS): Popcorn around the room to hear from the participants and write the answers to the questions on big paper. (Identify what themes are coming up, specifically the rules around data and sharing.

CLOSING (5 MINS)

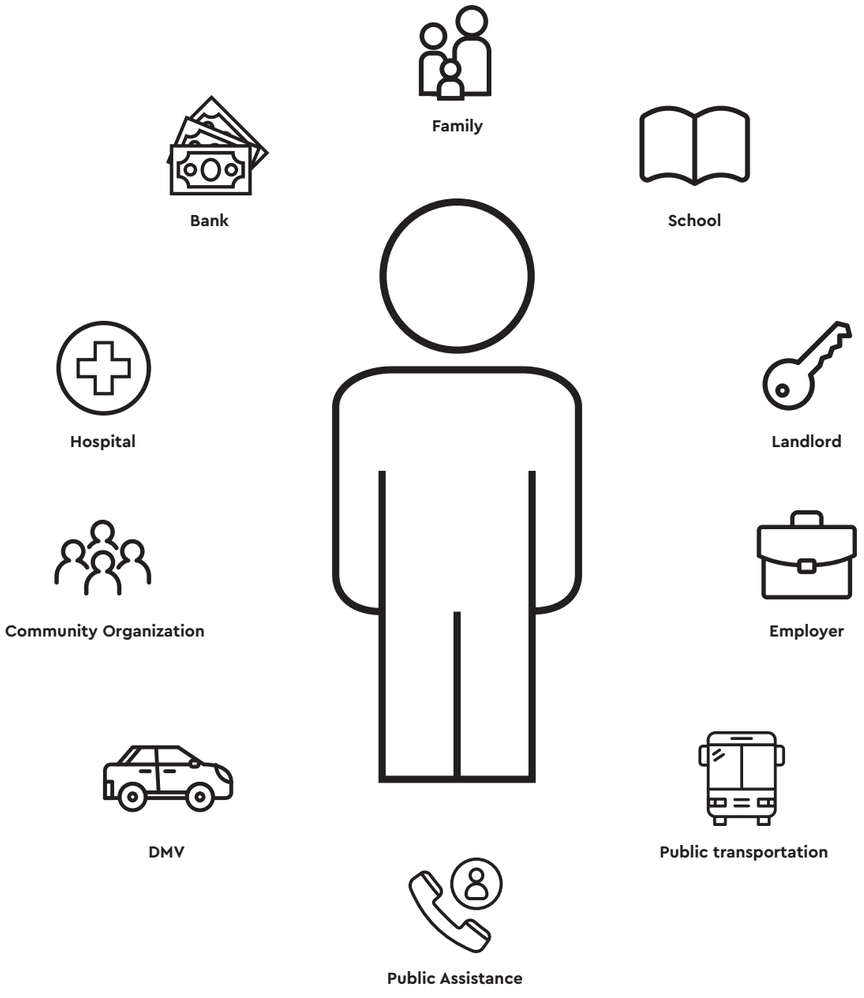
Say to participants, "It may be overwhelming to understand what and how much of our digital selves are being collected. But knowing is only the first step. Since we now have a better understanding of what's happening, we can protect ourselves and communities better."

Ask: "What are some ways you are currently protecting your digital information?" Popcorn around the room.

To close out, focus on our community defenses and talk about how we already have tools in our toolkits to protect ourselves, and how we are already doing the work. (Note: This may be a great time to hand out the "Tips for Data Self-Defense."(p.84)

WORKSHEET: Mapping Your Data Self

1. In the image of the body below, write all of the different types of digital information collected about you.
2. If two or more points of data are collected electronically by the service, item, entity, etc., draw connecting lines from the images surrounding your data body to your data body.
3. Draw connecting lines between the entities that share your information with each other. Examples: your school might collect your license plate information for pairing.



4. In the chart below, jot down some of the data, information, that is collected about you and write down how its collected.

Data Type	Who Collects it?	How is it collected /Stored?
Ex. License Plate	The city of Detroit	License plate readers, parking meter, toll booths

ACTIVITY: Data Profiling, Digital Decisions[6]

Time: 90 minutes **Group Size:** 5-25

OVERVIEW

This activity gets participants experiencing what it's like to be in the position of the profiler—someone who is tasked with making inferences or insinuations about who someone is based on their data.

GOALS:

- Get a sense of how easy or difficult it is to piece together who someone is based on a small piece of data
- Participants should come away thinking about the limits or strengths of creating a data profile about someone based on an aspect of their data trail

SUPPLIES:

Laptops, cellphones, or other devices with internet access (for conducting research); data set(s) from the list below; six envelopes that seal (one for each group); *Data Profiling, Digital Decisions* (p.67) Worksheet for each scenario; paper and pens

PREPARE BEFORE THE SESSION:

- A cell phone record for one month
- Utility bills for the past six months
- Purchasing history from Walmart.com
- A 24-Hour record of Google search terms
- A credit score
- Browser history from a recent browsing session

CONTENT

OPENING (15-20 MINS)

Say, "Welcome everyone. We're going to spend the next hour and a half role-playing as Data Agents, representing some of the roles we engage with in our everyday lives, like a financial services agent, a case examiner for Child Protective Services, and landlords. We will be using pieces of data about random people who are requesting our services or something similar from us."

6 Thanks to Virginia Eubanks for primarily developing this activity. It is also partly inspired by "But I Have Nothing to Hide! PRISM Break-Up Workshop," by Seeta Peña Gangadharan, Becky Hurwitz, and Emi Kane. Available at https://bit.ly/2yUJWYB.

INTRODUCTIONS (5-10 MINS): Go around the room and have each person introduce themselves providing their name, gender pronoun, community/organizaton they represent.

STORY SHARING (10-15 MINS)

In small groups have the participants answer the following questions: "Has a decision ever been made about you based on some digital information a company or person recived about you? How did it affect you?"

BEING DATA AGENTS (20 MINS)

EXPLAIN TO PARTICIPANTS: "Your job as a Data Agent is to try and figure the person out, including who they are, what they do or like, why they may do or like certain things, etc., in order to make a decision about their case."

Split the room up into six groups.

Hand out the information packets at random (they should be marked with different names but have the same information which includes: a month of call data (number, location, length of call) from the subject's cellphone, 2) utility bills for the last six months, 3) purchasing history from Walmart.com, 4) a day of Google search terms, 5) credit score, and 6) browsing history (a list of urls) for the person's last browsing session. Hand out a scenario card to each group. Instruct the participants to keep the packets sealed.

EXPLAIN THE EXERCISE: "Each group is now a "Data Agent" and decision-making team. Wearing the hat of the specific "Data Agent" roles you have been assigned, your team is to make a 3-4 sentence profile of this person and make a decision that is listed on the scenario card about the individual."

"Each team will need a note taker to write the profile of the person and complete the scenario card, and a reporter to report back to the entire group the decision made."

- "You will have 15 minutes after I tell you to open your packets to complete your mission. So you have very limited time. Be sure to split up the work to make best use of your person power."
- "Each team can use their personal devices so you can do some research and investigate any aspect of the subject that you think is needed. If it helps you, use Google maps or earth to look at places the subject has been. Research what books and movies they are browsing. Look up unfamiliar search terms. You are free to access anything that is public."
- "Ready? Open your packets and begin. Good luck."

REPORT BACK (20-40 MINS)

Say, "Welcome back everyone. I hope that was a productive little investigative session. I'd like to now ask you to give your judgments—not the demographic profiles, just the judgments—to the reporter that's affiliated with your group."

Ask for a group to volunteer to go first. Have their reporter read their scenario card, report back on their decision, and give an overview of the profile they created for the person. Continue until each group has gone.

Be sure they answer the following in their report back:

- "How exactly, did you make sense of the data trail on this person?"
- "What information stood out as most important and why?"
- "Were there any clues that made the person's race, gender, class, sexual orientation, or other demographics evident? On what basis?"

Facilitator's note: Once every group has gone, discuss some of the trends you noticed and ask the larger group what they noticed. For example, did everyone deny the request or accept them? Were folks hyper critical of the person? Etc.

After the large group discussion, inform everyone that they all received the same person's information, then reopen the conversation and dig deep into how the outcome and descriptions for each person was different and how that mimics our reality.

PROMPT: Say, "Often, people respond to the threat of data collection and profiling by saying, 'If you don't have anything to hide, you have nothing to worry about.' Take a minute to reflect on this, and write something down on the backside of a piece of paper from your packet."

GROUP DISCUSSION: Ask:

- "Did this activity challenge that way of thinking about for you?"
- "What do you think are appropriate responses from affected communities or political decision makers that are supposed to represent them?"

CLOSING (5-10 MINS)

Close out the group by collecting their demographic profiles, their verdicts, and their reflections. End by mentioning there are a lot of ways to consider opting out of data collection and by pushing for collective-level solutions, such as consumer privacy and anti-surveillance legislation. You can point them to info sheets in the "Community Defense Toolkit" (p.81) section of the Playbook.

WORKSHEET: Data Profiling, Digital Decisions

SCENARIO 1

You are a landlord of a rental property. You have just received an application from:

_____

(insert person's name)

Based on the documents you received, would you rent your property to this person? (Yes / No)

Why or Why Not?

_____

_____

Profile description:

_____

_____

SCENARIO 2

You are the manager at XYZ company. You have just received a job application from:

_____

(insert person's name)

Based on the documents you received, would you hire this person? (Yes / No)

Why or Why Not?

_____

_____

Profile description:

_____

_____

SCENARIO 3

You are a bank teller and you have just received a loan application from:

_____

(insert person's name)

Based on the documents you received would you give a loan to this person? (Yes / No)

Why or Why Not?

_____

_____

Profile description:

_____

_____

SCENARIO 4

You are a mother and are looking for a babysitter. You found a daycare center run by:

_____

(insert person's name)

Based on the documents you received would you enroll your child into the school? (Yes / No)

Why or Why Not?

_____

_____

Profile description:

_____

_____

SCENARIO 5

You are a Child Protective Services (CPS) case examiner who just received this case, you have been asked to determine if you should do a house visit and/or open a case against this person.

_____

(insert person's name)

Based on the documents you received would you visit this person's house? (Yes / No)

Why or Why Not?

_____

_____

Profile description:

_____

_____

SCENARIO 6

You are a National Security Agent who has been asked to determine if we open an investigation into this person as a potential threat to the security of the United States.

_____

(insert person's name)

Based on the documents you received would you open a case against this person? (Yes / No)

Why or Why Not?

_____

_____

Profile description:

_____

_____

POWER NOT PARANOIA!

ACTIVITY: Flip The Script

Time: 45-90 minutes **Group Size:** 5-25

OVERVIEW

Talking about data collection and data-driven systems in marginalized communities can be difficult, stir up raw emotions and memories, and cause people to experience paranoia and isolation. This workshop helps participants recognize their collective strength in identifying and practicing alternatives to oppressive, unjust data collection and data-driven systems.

GOALS:

- Reflect upon and share experiences with data collection and data-driven systems
- Identify different strategies for challenging oppressive data collection and data-driven systems
- Help draw out the collective power in communities to resist, refuse, or reorient the aims of and vision behind data collection and data-driven systems

SUPPLIES:

Quotes from the *ODB Quote Bank* (p.22) either written out on large index cards or printed on 8.5 x 11" paper; *ODB Themes* printed on 8.5 x11" paper (or larger); tape or blue tack; sharpie pens; butcher paper

PREPARE BEFORE THE SESSION:

Arrange the room "café style," so that people can work collectively in small groups. Place the quotes on tables.

CONTENT

OPENING (15 MINS)

INTRODUCTIONS (5-10 MINS): Go around the room and have each person introduce themselves providing their name, gender pronoun, community/organizaton they represent.

STORY SHARING (10 MINS): Have people pair up and answer the question: "Where was your mother's mother born?" Prompt people to switch after two and a half minutes. When both partners have gone, ask people to popcorn back what they learned and how that experience felt for them. When you've heard from at least three people, you can wrap the story share by referencing the power of narrating our own histories.

SHARING EXPERIENCES (30 MINS)

INTRODUCTION: Say, "During our research, the Our Data Bodies Project (ODB) team discovered several reoccurring themes about data collection, data-driven systems, and their impacts on the peoples' lives. Many of our interviews uncovered a feeling of paranoia or powerlessness, when interacting with data systems. We are seeking ways to shift that. In this activity, we introduce you to people who spoke with us and share their stories as a way of getting us to think about collective strategies for now and in the future."

SMALL GROUP ACTIVITY (15 MINS): Instruct people to:

- Select a reporter (someone who will report back to the large group) and someone who will scribe (e.g., write the themes);
- Read the quotes at their table, taking note of any reactions they have to reading the quote; and
- Identify (as a group) what themes does a quote or set of quotes point to.

Take about 15 minutes to do this.

If you feel the group needs it, you can introduce and pass out the worksheets as a way for people to reflect individually on their own experiences.

LARGE GROUP REPORT BACK (15 MINS): Ask, "Please share with us any report back from your group. What overarching theme or themes did your small group discover?"

FLIPPING THE SCRIPT (20-30 MINS)

Now have participants introduce a new narrative about data collection, data-driven systems, and their lives and needs.

SMALL GROUP ACTIVITY (15-20 MINS): Say to the room: "I want to invite you to move from paranoia to power. First, I want you to literally flip over the quote or quotes that you've been working with. As a group, think of an overarching theme or themes that is the opposite of the ones that your group just identified. Then, identify one thing you can do or one strategy you can embrace in order to make that theme a reality."

LARGE GROUP ACTIVITY (10-15 MINS): Go around the room and discuss each group's flipped script and strategies. Make sure to collect the strategies on butcher paper.

CLOSING (5 MINS)

Close with acknowledgment of the power in collectively identifying strategies to challenging harmful and unjust data collection and data-driven systems.

ACTIVITY: Systems In Our Lives

Time: 45-60 minutes **Group Size:** 5-25

OVERVIEW

This workshop builds on working knowledge of data systems and helps community members engage in a process of developing strategies to reclaim power of their data, bodies, stories, and communities.

By the end of this activity, participants should be comfortable in talking about systems that they confront in their daily lives and open to seeing themselves in other participants' experiences.

GOALS:

- Collectively answer the question: "What systems do we interact with on a daily basis as we go about accessing/exercising our human needs/rights?"
- Build community knowledge, create and practice ways to defend ourselves/rights, connect knowledge gained to our everyday lives, challenges, and work, and practice collective transformation and liberation with all participants

SUPPLIES:

Chairs, markers, sticky butcher paper, large sticky notes, camera (for documentation)

PREPARE BEFORE THE SESSION:

Think about setting up your room, so that it's easy to maneuver or move from one large group into small groups of about six people.

CONTENT

OPENING (20 MINS)

"Welcome everyone. We're going to spend the forty-five minutes or so thinking about the kinds of systems that we encounter in our daily lives and what that experience has been like for people. We'll start in large groups, and then branch off into smaller groups."

INTRODUCTIONS (10 MINS): Go around the room and have each person introduce them-selves providing their name, gender pronoun, community/organization they represent.

STORY SHARING (10-20 MINS)

In small groups have the participants answer the following questions: "What is one systems you had to interact with on your way to this workhop today? What information did it collect?"

IDENTIFYING SYSTEMS (10-20 MINS)

Get people seated in a large group at first and popcorn their thoughts on butcher paper, so everyone can see the entire landscape of systems that they collectively interacted with. If you're able, have an accessible layout that allows people to move from their large group seats (say a U shape) to smaller circles, where there are wall surfaces and supplies. Have sticky butcher paper ready for small group break-outs after the large group discussion.

Large Group Discussion: As a group, brainstorm and map out answers to the following questions and capture themes on the butcher paper:

- "What are systems?"
- "What words come up when you think of systems?"

Capture people's answers on the butcher paper. After 5 minutes or so, ask:

- "What do they have in common?"
- "How are they different?"

Digging Deeper: On a new sheet of paper, ask people to brainstorm and map out answers to the questions:

- "What are some systems that you encountered in the last twenty-four hours?"
- "In the last week?"
- "Which of these systems could you group or link together, and why?"

Do this until you have few enough groups that you could divide people up into small groups.

Focusing Down: If you need to probe and get people to identify systems more specifically, you can offer questions such as:

- "What are public benefits systems?"
- "Which systems are we most frequently interacting with in our contexts?"

Capture these on butcher paper, underline or graphically offset items that people call out, and get people to help you group these systems, in case you need to cluster people into a small group with several systems.

NAMING SYSTEM HARMS, BENEFITS, NEEDS (20-30 MINS)

Small Group Discussion: Next, get people to divide into small groups of no more than six according to their system of preference. You will need to repeat back the names of the systems people discussed, first, and then allow people to sit in their groups. Be sure to prompt each small group for a recorder and someone who might feel comfortable reporting and/or ready to report back to the large group. Remember to leave space for people to put their small group notes on a wall where the other large group notes are laid out.

If there are space limitations or other limiting factors, ask people to pair up. If you're unable to have small group discussions, get people to pair up and just use large sticky notes or large index cards that they would be willing to affix to a wall for others to see.

Once people are in small groups or pairs, say, "Now that you are in the small groups, I'd like to offer four questions for discussion.

- What was your experience with this system or these systems?
- How did that make you feel?
- What do you know about how our information is collected, shared, or used when we interact with this system or these systems?
- What "don't you know" or do you want or need to know about this system or these systems?"

For all of these questions, instruct a note-taker to capture themes on butcher paper. Then instruct people to put their butcher paper or large sticky notes on the wall.

CLOSING (10 MINS)

Do a gallery walk and get people to popcorn similarities and differences. Additionally, ask participants to:

- Share one word that represents how they are feeling right now. (e.g., powerful, confused, supported, challenged, etc.).
- Use their body to express how they are feeling right now.
- Share one thing they are taking with them from the workshop.
- Share something they learned that they want to share with someone else.
- Share something about their community that they are grateful for.
- Share a question that came up for them.

Document all the questions, and address them in future sessions or community-based research.

Alternately, transition to "Systems Between Us" (p.79) using opening prompt.

ACTIVITY: Look Up!
What's in Your Community?

Time: (Part 1) 45-90 minutes; (Part 2) 60 minutes; (Part 3) 45-90 minutes
Group Size: 5-25

OVERVIEW

There is evidence of a "stalker state" all around us, especially in neighborhoods and communities that are in conditions of poverty, experiencing gentrification and criminalization in their daily lives. In this activity, we document different kinds of surveillance tools used by state and private actors.

GOAL:

- Create awareness of both state and corporate surveillance that is taking place in our neighborhoods and to begin thinking of ways to make neighborhoods free from unwanted surveillance

SUPPLIES:

Clipboards; notebook or notepad; pens, pencils, markers, and/or color pencils; print outs of Google maps; printers; smart technology to take pictures

PREPARE BEFORE THE SESSION:

If you need to, you can split up this activity, so that you organize and instruct participants to carry out Parts 1 and 2 on different days. Also, you may find it useful to consult the *Community Bag-of-Tricks* (p.90), which contains additional resources, including an example of a surveillance walk in Oakland, California, as well as Stop LAPD Spying Coalition's "Watch the Watchers. They Lie!" film. Play around with the features of Google maps in order to help participants navigate and learn how to use it.

CONTENT

PART 1. OPENING (30 MINS)

INTRODUCTIONS (15-20 MINS): Have participants go around the room and introduce their names, their gender pronouns, the community/organization they represent, and a sentence or two about what they love about the neighborhood they're from.

STORY SHARING: (5 MINS): Take a minute, close your eyes, imaging that you are

walking in your community, think about the things you hear, see, feel, taste, smell. Take 2 minutes to write your thoughts down.

REPORT BACK (5-10 MINS): In pairs, have participants discuss some of the things they envisioned. Popcorn around the room to hear what folks have to say. Ask the question: "Using a show of hands how many people imagined or envisioned surveillance technology?"

IDENTIFYING NEIGHBORHOODS (15-20 MINS)

Based on the story share, ask participants to pair up, so that two people are covering the same neighborhoods/ area.

Introduce participants to Google maps, including how to search for neighborhoods and take screen shots, taking the time to walk them through this part of the activity if they are unfamiliar with technology.

Have participants print out their neighborhood maps on at least an 8.5 x 11" size paper (bigger 11 x 17" is also good).

IDENTIFYING DIFFERENT TYPES OF SURVEILLANCE (40-45 MINS)

During this community walk we will be primarily identifying the types of state and corporate surveillances in our communities.

STATE SURVEILLANCE (15 MINS): Explain that state surveillance refers to surveillance tools used by state agencies.

1. Ask participants to identify, popcorn style, what they know about surveillance technologies in their neighborhood. (Take notes on large paper for the group to refer back to.) It is often easiest to begin with CCTVs or traffic cameras.
2. Have participants conduct image searches for each technology so everyone can see what different surveillance technologies look like. Say, "Take a few notes about these different forms of state surveillance on the back of your map, so you can remember to take pictures of these when you're out on the street."
3. Move on to corporate surveillance.

CORPORATE SURVEILLANCE (15 MINS): Explain that corporate surveillance refers to surveillance tools used by private actors, likes stores and shops. They can be cameras used by the local corner store to signs of "No trespassing, private property" to predatory advertising (also known as "bandit signs"), such as signs that say "Need cash? We pay cash for homes."

1. Ask participants to identify, popcorn style, some locations they have seen these examples and ask if they know about additional types of Corporate surveillance technologies in their neighborhood. (Take notes on large paper for the group to refer back to.)
2. Have participant's conduct image searches for each technology so everyone can see what different surveillance technologies look like.
3. Have participants take a notes about these different forms of corporate surveillance on the back of their map, so they can also remember to take pictures of these when they are out on the street.

COMMUNITY KEY (10 MINS): In pairs, ask participants to review the notes they took and what they've just learned. After reviewing the different types of technologies, have them create an icon list for each identifiable technology. For example, draw an eye for security camera installed by a business, pig for police camera, rectangle for predatory ads/bandit signs, circle with line through it for no trespassing.

Facilitator's Note: The icons should be easy to draw, and participants should keep a list for them to review later on.

PART 2: SURVEILLANCE WALK (30-60 MINS)

Send participants out in pairs to document surveillance in their neighborhoods.

Before Hitting the Streets Instructions (5 mins):

1. Each pair/group will be canvassing the community together.
2. In each group, there needs to be a photographer and note taker.
3. The note taker, using the icon key created, will document where the technology is on the maps.
4. The photographer will take an actual photo. For each picture they take, they should take note of the location, and the type of surveillance (state or corporate), any observation they might have.
5. Pairs should also look for anything new or different—i.e., document images of any forms of surveillance that were not previously discussed.
6. Encourage pairs/groups to speak with business owners, community members, or others as they are documenting images in their neighborhoods.

Facilitate Notes: Groups and pairs should not split up, should not enter properties that have "no trespassing signs," and if they feel treated should meet back at the safety pick up location and call the facilitator.

PART 3: MAPPING SURVEILLANCE IN OUR NEIGHBORHOODS (45 MINS)

MAPPING (20-30 MINS): After bringing the pairs back into the room, get them to review, make notes, and mark up their neighborhood maps based on what they took pictures of and where. When the mapping is done, you can ask each pair to put up their map on a wall, where people can easily view the map.

DISCUSSION (15-20 MINS): Ask participants the following questions:

- "What's the overall look of surveillance in your community?"
- "What patterns are you seeing?"
- "Are there any differences between the neighborhoods that people mapped?"
- "What might these maps look like in a different part of town, for example, in more affluent neighborhoods?"

CLOSING (5-10 MINS)

Encourage your participants to document their maps and think about how to share them with others. Ask participants:

- "What resonated with you the most about this activity? What can you begin to change or demand of business owners, police, or policy or decision makers in their communities?"
- "What is one way you will share this information with your community members and communities?"
- "What are some demands and/or policies you think should be put into place to help protect your communities from more surveillance?"

You can introduce the ICU Oakland case and their successful protest against the construction of a massive surveillance control center (i.e., fusion center) in their community. As well, you can also screen the whole or excerpts of Stop LAPD Spying Coalition's "Watch the Watchers" as what this type of community walk can develop into. See the "Community Bag-of-Tricks" (p.90).

ACTIVITY: Systems Between Us

Time: 45-90 minutes **Group Size:** 5-25

OVERVIEW

This activity should follow the "Systems In Our Lives" activity, which asks people to name data collection or data-driven systems that they encounter daily. "Systems Between Us" is meant to be a kinetic experience, with people physically building a web of strength that binds them together. It draws on similar pop-ed activities that show how people can network with one another and build a base that can inform collective action.

GOAL:

- See and hear how we experience the same data-driven systems
- Recognize our shared experiences are a source of strength and collective action

SUPPLIES:

Yarn

PREPARE BEFORE THE SESSION:

Remember that this activity works best when it is preceded by *Systems In Our Lives* (p.72).

CONTENT

OPENING (5-10MINS)

"Hi everyone. We're going to transition to talk about our shared experiences with different data-driven systems."

Facilitator's Note: If you are starting this activity without having done "Systems In Our Lives," (p.72) please pick an introduction and story sharing activity from elsewhere in the Playbook.

CONNECTING THE DOTS: BUILDING COMMUNITY (20-30 MINS)

Say, "We'd like to invite you to rearrange your seats from the small groups to the large groups."

After everyone has readjusted their seating, say: "For this next activity, we're going to use

a popcorn format. You can think of yourself as a speaker or a listener. At any time, you want to be the speaker, feel free to volunteer the name of a system that came up in your group. Please make sure everyone can hear you."

Elaborate the instructions:

1. "First, name the system."
2. "Second, describe the experience your group talked about. I'll hand you the ball of yarn."
3. "If you're listening in, and you also talked about that particular system, please raise your hand. Keep your hands up high, so we can see you."
4. "Whichever speaker has the ball of string, please select someone who raised their hand to toss the string to."
5. "Then that person will go, and state the name of the system. They will state their own or the group's experience with that system."
6. "When they've finished, then they toss the string on to the next person who has their hand up, and so on and so on."
7. Then begin the activity.

CLOSING (5-10 MINS)

Say, "Now that we've gone through the different systems that each of you discussed in your small groups and charted these discussions among us, we can see the connections between us. We honor each of our individual experiences and also notice that we are not alone, we are experiencing systemic issues. By naming these systemic connections between us we can build/share power to challenge and transform them. We are stronger together."

Safety vs Security: Are You Safe or Are You Secure?

by Tawana Petty

Unfortunately, when people think about security, they often equate it with safety. The synonymous use of these terms can cause harm to those at the end of the systems designed under this conflation.

Security is not inherently safe. In fact, most times security is on the opposite side of the spectrum. When people think of security, they are typically thinking about securing items, property, or even their identity. Very often, this mindset does not have a human factor involved. To be safe, can mean to be secure, but to be secure does not necessarily mean a person is safe. We install security systems on our homes to protect our property. We advocate for security cameras on police officers in order to hold accountable those officers who engage in police brutality, and we add security alarms to our vehicles in hopes that we deter theft. Although these mechanisms may provide us with a temporary measure of comfort, they have proven time and time again that they do not increase our safety. An alarm system cannot ensure an individual is protected from actual harm, just as a body camera cannot prevent police brutality. The ways we talk about safety and security are important as we think about the healthy digital ecosystem we hope to create.

There is no magic spell that can guarantee our safety. There will always be circumstances outside of human control that put us at risk. However, as we think about data systems and technology, there are measures we can take to increase our safety and maximize our security. We can add tools such as Signal or a VPN to make our technology more secure, but in order to make our interactions—digital and otherwise—safer, they must be connected to a healthy digital and non-digital ecosystem. If a person sends an encrypted text message and the user on the other end is also encrypted, chances are the communication is secure. However, if the person on the other end is not a trusted comrade, the level of security added to the technology holds little relevance. This is the mindset one must have when engaging in digital security and data safety.

Often, for undocumented, black communities and other marginalized communities, the safer a city proposes to be, the less safe those communities become. When cities invest in the security of neighborhoods by adding surveillance cameras and increasing the militarization of police departments, it poses an imminent threat to those residents who are often deemed expendable. The security mindset without the human element is inherently unsafe.

One of the ways we can increase our safety, is by nurturing relationships. This applies to online and offline communication. A neighbor who regularly communicates with other neighbors has a greater chance at being safe than a neighbor who has no one looking out for them. Neighbors who have agreed to turn on their porch lights in order to keep their streets lit and lookout for one another are engaged in nurturing safety. This is different than adding a security system which is meant to protect your property and belongings.

These methods of fostering a safe community are also essential to our online communication. A person who experiences unsolicited spam or damaging images or communication via email or on social media receives greater protection when there is a community of people looking out for them. Once they are alerted by their online community about the breach, they can increase their security by changing their password. The online community may also engage in collective action, such as reporting the spammer to social media administrators. This creates a safer online environment.

PRINCIPLES

Some of the ways in which we can help to foster a safe digital ecosystem is through the implementation of the Detroit Digital Justice Principles (access, participation, common ownership, healthy communities) and the Equitable Internet Initiative Principals (collaborative problem solving, storytelling, education, collaborative community ownership and governance, long term, authentic relationships, and alternative energy). The principles can be found in detail at Detroit Community Technology Project's website detroitcommunitytech.org.

By nurturing a healthy digital ecosystem, we help to ensure the safety of those we engage with, whether on the computer or in the neighborhood.

It is important as we go about doing the work of creating the world we wish we live in, that we do not conflate what makes us safe with what it takes to be more secure. In all we do, the human element must be part of our daily interactions.

Tips for Data Self-Defense

By Virginia Eubanks

While every system is different, there are some basic strategies you can use to protect your personal and community data from abuse:

Always ask: Is my social security number necessary? In many systems, you can be assigned a unique client identifier (UCI) instead of a social security number, especially if you are a victim of domestic violence. This will protect your identity somewhat, and will make it more difficult for your information to be linked up across systems. However, for systems that require verification of assets and income—like TANF, General Relief, or SNAP—you will almost always have to give a social security number to qualify for benefits

It's not all or nothing: In many cases, public programs will accept applications that have some sections crossed out. Tell a caseworker if there are any sections of an application or parts of an interview that make you uncomfortable. Ask, "If I choose not to disclose that information, will it impact my chances of receiving benefits?" If the answer is no, cross that section out!

Always appeal: If you are rejected for or terminated from a public program, immediately request an appeal of the decision (often called a fair hearing). Always request the fair hearing in writing. Always request that the fair hearing be held in person (not over the phone). In many programs, like SNAP, TANF, and Medicaid, filing an appeal will protect and maintain your benefits until a hearing can be held. However, if you lose your appeal, you will be liable for the cost of the benefits you receive—you'll have to pay them back.

It's not forever: Ask if there is an "expungement" process available. Expungement means that, after a certain amount of time, your record is "sealed" (can't be opened or read by anyone) or removed entirely from a system. For example, in many states, a CPS record that indicates child abuse or neglect can be sealed 10 years after the involved child's 18th birthday. Youthful offender criminal records can often be expunged as well.

Always document: Documents often get lost, and it is almost always seen as the applicant's fault when something goes missing. Keep a copy of EVERYTHING you send to a public program. When possible, ask that anything you submit be stamped "received" and request a copy of the confirmation that it has been submitted.

Request your record: Based on legislation called FOIA/FOIL (Freedom of Information Act/Law) or PRA (Public Records Act), you can request copies of public records—including your own—from federal and state agencies like HUD, Department of Corrections, etc. It's your record. You should be able to see a copy of it.

Credit Score, Credit Report: What's It Got to Do with Me?

By Kim Reynolds and Seeta Peña Gangadharan

CREDIT SCORES

Are one of the most prevailing risk assessment tools in our society. Lending remains the main use of credit scores, and they are a gateway to a mortgage, car loan, college loan, credit card, and more.

You receive a score based on your credit report (see below). To lenders, a high credit score means you are a low risk, are likely to get a loan or other service, and will have lower interest rates or better terms of repayment. A low credit score reads less favorably to lenders, which could result in not getting a loan or other services, or paying more for such services. In other words, people with "bad credit" may be charged a higher interest rate for any kind of loan, or denied a loan altogether.

There are many problems with relying on credit scores for lending. The use of credit scores is precarious, lacks context, and can seriously injure those with bad credit. Moreover, bad credit or lack of credit history often results of from a history of structural discrimination. In a country like the United States, where medical bills add up rapidly, where racial and gender discrimination locks people out of opportunities, and where low-income people and families face expensive barriers to bettering credit, no or low credit scores can interfere and greatly affect your life.

In cases where low credit scores result in a bank rejecting a request for a loan, many people turn to payday or quicker means of securing loans, which are often predatory in nature. These institutions charge incredibly high interest rates on even small amounts of money.

Nowadays, cell phone providers, insurers, utility companies, and landlords use credit scores for non-lending purposes, including to set interest rates, determine the size of deposits, or decide whether one gets a contract. Renters with a low credit score may have difficulty renting an apartment. In some states, people with poor credit may have to pay a security deposit to get basic utilities like electricity, and some cell phone companies will deny people based on poor credit.

For any person facing a poor credit score, the path forward is difficult, leading many to feel stuck in a vicious cycle. The ways to improve credit are difficult (such as bankruptcy),

and low credit can spell high risk for employers, meaning discrimination against people with low credit scores can be high.

Credit Reports and Getting (or Keeping) a Job

In our current job market, credit reports loom large, and future and current employers frequently ask your permission to run a credit report check. Whether for a top-level job or entry level position, employers typically hire employee background check companies who purchase credit reports from anyone of the big credit reporting agencies: Experian, TransUnion, and Equifax.

A credit report contains information such as your bill-paying history, length of your account with a company, any outstanding debt you have, any unpaid debts that have been registered with a court, any public record of having been sued, gone bankrupt, or failed to pay taxes (tax lien), and history of debt collection against you. Like the credit score, credit reports tie to a longer history of structural discrimination that includes predatory targeting of people for risky financial products (payday or short-term loans) and to limited opportunities to build or rebuild credit.

On top of discriminatory and predatory practices that link to bad credit, credit reports suffer from inaccuracies, for example due to identity theft. Inaccuracies or unidentified identity theft can leave some stuck in a loop of being denied a job.

FACTS AND MYTHS ABOUT CREDIT REPORTS

This fact and myth sheet can hopefully help navigate what a credit report is, what it is used for, and what your rights are as an applicant and employee.

I can be denied a job based on my credit report. Fact and Myth. You unfortunately can be denied a job based upon your credit history in 39 states. This generally is expressed in a written letter. Eleven states (California, Connecticut, Hawaii, Illinois, Maryland, Oregon, Vermont, Delaware, Nevada, Colorado and Washington) plus the District of Columbia all ban the use of credit as a discriminating or evaluating factor in employment practices (but can still request and pull your credit history). Therefore, this statement is a myth in 11 states, where you cannot be legally discriminated against for your credit history in employment processes.[1]

I have to give my permission to an employer to run a credit report check. Fact. Under the Fair Credit Reporting Act, employers must obtain written consent from you as an employee or applicant to run a credit report check.[2]

"Bad credit" or lack of credit affects 50% of Americans. Fact. According to the Consumer Financial Protection Bureau, 26 million adults in the US do not have established or documented credit history with the three major credit reporting agencies mentioned above. Additionally, over 50% of the American population have sub-prime credit scores (scores under 720) and one in three have a score lower than 630.[3]

I shouldn't apply for a job if I think my credit will be a problem. Myth. In 11 states in the US, there are state laws that restrict or attempt to limit the use of credit reports in the employment process. However, if a credit report check is run in state in the United States, the employer must notify you of what is called "adverse action" where they will terminate the application due in part to one's credit history. Applicants can then dispute this if they feel their credit report isn't correct. Some background checks companies that run credit reports allow users to add context notes as well that are visible to the employer, allowing applicants to give context to something that could be potentially considered a red flag.[4]

Credit reports are good way to assess my employability. Myth. Credit reports were designed for lenders to evaluate systematically, and not for employers. According to Prosperity Now, "In most cases, credit checks are an improper tool for assessing employee liability and constitute an unfair barrier to employment for those with poor credit histories — those who are often most in need of a good job."[5]

Bad credit can be difficult to improve. Fact. Say your family experiences a medical emergency and your healthcare does not cover it all. Say you're someone who has experienced violence (especially as a woman) or someone who has developed a condition that requires regular hospital visits. If you do not have the resources to pay these bills upfront, the outstanding debt with medical institutions can take a toll on your credit. Means of improving credit through obtaining better credit can also be difficult in that higher interest rates may accompany a loan or credit card.

Employers see my credit score. Myth. When an employer conducts a credit check, they do not see your credit score. Rather, they access your credit report, which details your credit history such as loans or bankruptcy.

Data Brokers and Opting Out

By Kim Reynolds and Seeta Peña Gangadharan

In the adaptation of moving so much of our lives online, private and public companies have also adapted, however, sometimes with dangerous consequences. The data broker industry is one that is diverse and far reaching. Data brokers are often associated with buying and selling your online shopping history to marketers, but data from all kinds of online and offline activity can be bought and sold, with serious repercussions.[6] This info sheet outlines the research we have done around the buying and selling of data like phone calls made to prisons, cell phone location, medical records and prescription histories, public or sealed records, and social media activity and how this can affect marginalized bodies.

What is a data broker? A data broker is an entity or individual that aggregates, analyzes, and buys and/or sells data that is related to both online and offline activities.[7] The work of a data broker can depend on the social domain they focus on, such as commercial interests, consumer interests, geolocation, or medical records.

How do they work? Data brokers have existed long before the internet, but the internet and very few regulations that determine what companies can and cannot do with your data online have fueled their growth. Data brokers buy and sell a myriad of information from anywhere from online shopping history, to Facebook posts, and even individual records of Walgreens prescriptions to sell to pharmaceutical research labs or other profile assembling brokers.[8]

This kind of data brokering both overlaps and differs from what is known as consumer reporting agencies. When data are used for decisions about credit, employment, insurance, housing, and other similar eligibility decisions, the Fair Credit Report Act applies and ensures some safeguards for consumers.[9] But FCRA does not cover the sale of consumer data for marketing and other purposes—i.e., the business of many data brokers.[10] Some data brokers, such as Experian, overlaps both as a data broker and as a consumer reporting agency.

What are the concerns and risks? Data brokers and their practices can have serious privacy implications for any person, but for marginalized and vulnerable citizens the buying and selling of our information by data brokers also ties to problems of predatory targeting, racial profiling, and discrimination by the state and corporations alike.

For example, a 2013 report by the U.S. Senate Commerce Committee revealed that companies that provide financially risky products such as high interest payday loans were buying profiles of financially vulnerable people from data brokers who created such profiles.[11] This information was then used in the marketing for "subprime" products (i.e., products aimed at people with bad or no credit), which in turn increases people's risk for spiraling into financial debt.

Major data broker companies such as Spokeo, Experian, and Tracers keep records and create databases on personal data such a criminal records, addresses, email and telephone information, which can also target returning citizens if these profiles are used for police surveillance, a practice Tracers specializes in. Additionally, data brokers such as Location Smart and Geofeedia sell geolocation and social media information to clients including law enforcement. Such information facilitated the targeting of Black Lives Matter activists during the uprising in Ferguson, MO.[12] The targeting of citizens and activists cost a police department in Boise, Idaho $24,000 in 2015 for a yearly subscription to Snaptrends, which boasted to aid the department to learn a suspect's "geographic patterns of life" through Twitter activity.[13]

What can I do? The best advice data privacy experts is to attempt to opt-out from data collection whenever possible. Deny the use of your location on apps, uncheck the boxes on sites to receive subscriptions offers from third parties, and opt out of pre-approved credit offers.[14] Become familiar with digital security tools and practices, too. For example, the Web browser DuckDuck Go has built-in features to prevent other third parties from tracking a user's web browsing activities. Free messaging app Signal encrypts your messages "end to end," meaning that only your device and the device of your recipient can read your message. Ad blockers can also limit the tracking of your Web behavior. These individual-level actions can reduce some aspects of state and corporate surveillance as well as heighten your own awareness of your online presence.[15]

What we can we do collectively? You can also mirror local abolitionist efforts like those led by the Stop LAPD Spying Coalition, which regularly documents information sharing of the stalker state. (See our "Community Bag-of-Tricks" (p.90) for the link). Groups like Center for Democracy and Technology (CDT) and and Electronic Privacy Information Center (EPIC) focus on broader legislative campaigns to reform commercial data collection and use.

Our Community Bag-of-Tricks

In our many workshops across the United States and in other countries, we have learned a lot from our participants who are already developing, practicing, or keeping tabs on different resources for community members who are trying to navigate and challenge data collection and data-driven systems. Here is a list of many of them. Check the Our Data Bodies website for a fuller list, and please email us and/or tweet out any other relevant resources so that we can grow this list and share far and wide.

ARCHITECTURE OF SURVEILLANCE — EXPLAINED
Stop LAPD Spying Coalition

A worksheet on different facets of the surveillance state.
https://bit.ly/2DI05ol

BAN THE BOX: U.S. CITIES, COUNTIES, AND STATES ADOPT FAIR-CHANCE POLICIES TO ADVANCE EMPLOYMENT OPPORTUNITIES FOR PEOPLE WITH PAST CONVICTIONS
Beth Avery and Phil Hernandez, National Employment Law Project

A lengthy report that details all fair chance hiring laws across the nation
https://bit.ly/1dfQy6N

BUILDING CONSENTFUL TECHNOLOGY
Una Lee & Dann Toliver, And Also Too

A zine published in 2017 that "is intended for anyone who uses, makes, or is affected by digital technologies and wants to build a more consentful world."
https://bit.ly/2gLR8Rg

COMMUNICATION IS A FUNDAMENTAL HUMAN RIGHT. ISSUE #2
Detroit Digital Justice Coalition

A 2010 zine that contains the Detroit Digital Justice Coalition principles.
https://bit.ly/2qm0JiB

DIGITAL SECURITY
Tactical Technology Collective

Digital security tips and trainings for activists.
https://bit.ly/2zOxFnI

ELECTRONIC MONITORING IS A FORM OF INCARCERATION
Center for Media Justice

A 2017 fact sheet on electronic monitoring.
https://bit.ly/2yEFFbN

EM FACT SHEET 2017
Challenging E-Carceration: Voice of the Monitored

A 2017 fact sheet on electronic monitoring.
https://bit.ly/2P5K6GH

EQUITABLE OPEN DATA REPORT
Detroit Digital Justice Coalition and Detroit Community Technology Project

A 2017 report on recommended guidelines for open data projects at the city or municipal level.
https://bit.ly/2PD2y90

FACT SHEET ON SOCIAL MEDIA ACCOUNTABILITY
Center for Media Justice

Eight facts about social media and their influence, as well as some suggested solutions.
https://bit.ly/2DfsLoC

ICU OAKLAND: SURVEILLANCE CAMERA WALKING TOURS AND ANTI-SURVEILLANCE COMMUNITY ORGANIZING Sarah Reilly (Design Action Collective), Salima Hamirani, Jesse Strauss (Coalition for Justice for Oscar Grant), Bex Hurwitz (RAD/MIT Center for Civic Media), Mark Burdett (EFF), Emi Kane (Allied Media Projects)

An example of a surveillance walk, where participants walk around different neighborhoods, identify surveillance cameras in their neighborhoods, and map their location. Written in the context of organizing and activism around the planned (but eventually aborted) construction of a fusion center in Oakland, CA.
https://bit.ly/2EWoF6m

INFORMATION SHARING ENVIRONMENT: "STALKER STATE"
Stop LAPD Spying Coalition

A visual map of different government institutions that share data with one another.
https://bit.ly/2QsfYSN

INTERNET FREEDOM AND DIGITAL SECURITY
Equality Labs

Digital security training grounded in principles of equity and justice.
https://bit.ly/2A1MkMU

POWERNOTPARANOIA.MD
Ken Montenegro

A basic overview of a digital security curriculum developed by Ken Montenegro, one of the co-founders of Stop LAPD Spying Coalition.
https://bit.ly/2Ojt7f0

ROBOT HUGS
RH

A blog about identity.
https://bit.ly/1cjUJWF

SECURITY PLANNER
Citizen Lab

A comprehensive set of tools and practices you can use to better protect yourself online.
https://bit.ly/2OZ3jtL

SURVEILLANCE OF IMMIGRANTS AND MUSLIMS
Center for Media Justice

Six facts about surveillance practices and industry with respect to Muslims and immigrants.
https://bit.ly/2DGYkHX

THE CALIFORNIA FAIR CHANCE ACT: KNOW YOUR RIGHTS AS A JOBSEEKER UNDER THE NEW "BAN THE BOX" LAW
National Employment Law Project

A worker fact sheet regarding new California fair employment rules, which serves as a potential model.
https://bit.ly/2zhP3S4

THE PRIVACY PARADOX: NOTE TO SELF
Manoush Zomorodi (Host)/WNYC

A WNYC radio series that explains different facets of your digital identity, privacy complications, and different ways to protect your data.
https://bit.ly/2kSGjx5

WATCH THE WATCHERS. THEY LIE!
Stop LAPD Spying Coalition

Based on community research, a short film about police surveillance used in Los Angeles.
https://bit.ly/2OeHMIg

WHAT ARE STINGRAYS?
Color of Change

A one-pager description of stingrays (otherwise known as IMSI catchers) and their surveillance capacities. Written in 2017.
https://bit.ly/2AFuQaX

EVALUATION

It is useful to have a set of standard questions that you ask after either a whole workshop or a particular activity. Getting feedback from participants will help you improve the activity for the next time and connect with your communities more effectively.

As a general rule, we suggest that you pose three basic questions to participants. They are:

- What worked well about this session/workshop?
- What didn't?
- What might you do differently or change about this workshop?

As an optional follow-up question, you can ask:

- What of this workshop/activity do you plan to take back to your communities?

After our workshops, we typically sit down and self-evaluate as well, by asking ourselves the same questions. We suggest you do the same and also take the time after a session to document notes, drawings, butcher paper, and other artefacts.

CLOSING REFLECTION

Our collective efforts to improve our data rights and work towards data justice are growing every day. We hope this Playbook will serve as one of many resources that can help sustain and nourish our movements.

As we move forward with this work, we invite you to share any pictures, quotes, notes, or resources with us and our larger communities.

Please feel free to email these to us at
info@odbproject.org or Tweet at #OurDataBodies.

ENDNOTES

1 Amy Traub, *Discredited. How Employment Credit Checks Keep Qualified Workers Out of A Job* (New York: Demos, 2013), https://bit.ly/2Pxswek

2 *Fair Credit Reporting Act* (Experian, n.d.), https://bit.ly/2QiHfGQ; *A Summary of Your Rights Under The Fair Credit Reporting Act* (Washington, DC: Consumer Financial Protection Bureau, 2015), https://bit.ly/2Ap0xH5.

3 *Credit Fact File* (Washington, DC: Prosperity Now, 2016), https://bit.ly/2OhXlPp; *Whose Bad Choices? How Policy Precludes Prosperity and What We Can Do About It* (Washington, DC: Prosperity Now, 2018), https://bit.ly/2yM7sXQ.

4 Susan Johnston Taylor, *Can Bad Credit Ruin Your Job Search?* (Bankrate, 2011), https://bit.ly/2RuJZBq

5 *Credit Fact File*

6 Yael Grauer, *What Are "Data Brokers,' And Why Are They Scooping Up Information About You?* (New York: Motherboard, 2018), https://bit.ly/2AADXt7.

7 Yael Grauer, What Are *"Data Brokers"*

8 Kalev Leetaru, *How Data Brokers And Pharmacies Commercialize Our Medical Data* (New York: Forbes, 2018), https://bit.ly/2AEwDwF.

9 *Data Brokers. A Call For Transparency And Accountability* (Washington, DC: Federal Trade Commission, 2014), https://bit.ly/1AwePQE.

10 *FCRA Summary of Rights,* (Equifax, n.d.), https://bit.ly/2DgiJ6w.

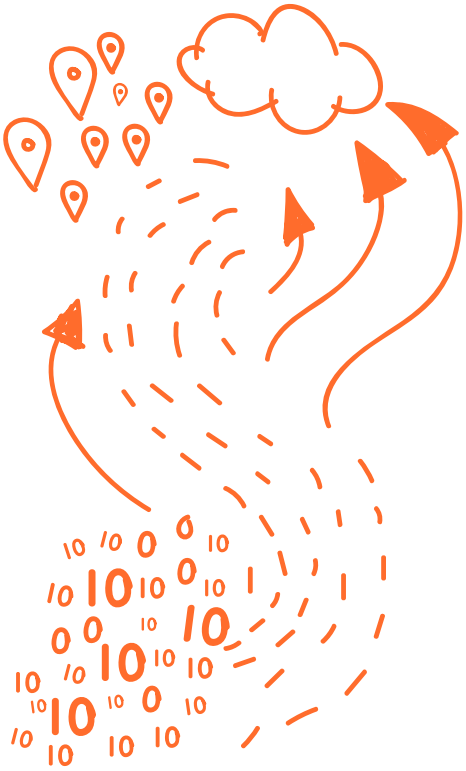
11 Aaron Taube, *How Marketers Use Big Data To Prey On Poor* (Business Insider, 2013), https://read.bi/2zoIo8C; What Is A FICO Score? (Washington, DC: Consumer Financial Protection Bureau, 2016), https://bit.ly/2CV8zHx.

12 Matt Cagle, *Facebook, Instagram, And Twitter Provided Data Access For A Surveillance Product Marketed Towards Activists Of Color* (ACLU Northern California, 2016), https://bit.ly/2dafbRD.

13 Ben Elgin and Peter Robison, *How Despots Use Twitter To Hunt Dissidents* (Bloomberg, 2016), https://bloom.bg/2dPHMMr.

14 *Opt Out List* (Stop Data Mining Me, n.d.), https://bit.ly/2AEV2T2; Data Brokers (Privacy Rights Clearinghouse, n.d.), https://bit.ly/2CQEBo9.

15 *Security Planner* (Citizen Lab, 2018), https://bit.ly/2OZ3jtL



info@odbproject.org
https://www.odbproject.org
#OurDataBodies