



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



# **COMMUNITY DEFENSE TOOLKIT**

This zine is an excerpt from *Our Data Bodies: Digital Defense Playbook*. You can find it at the following URL: <https://www.odbproject.org/tools/>



## Contact Info

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

## Copyright Info



This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of Our Data Bodies content when proper attribution is provided. This means you are free to share and adapt ODB's work, or include our content in derivative works, under the following conditions:

Attribution: You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit [creativecommons.org](https://creativecommons.org).

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.

## COMMUNITY DEFENSE TOOLKIT!

# 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>.

# 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](mailto:info@odbproject.org) or Tweet at [#OurDataBodies](https://twitter.com/OurDataBodies).

## COMMUNITY DEFENSE TOOLKIT!

## 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](http://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.

## COMMUNITY DEFENSE TOOLKIT!

### 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>

**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/2QsfY5N>

**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>

# 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).

## COMMUNITY DEFENSE TOOLKIT!

# 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/2DIO5ol>

## 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/2qmQjIB>

## 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>

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.<sup>11</sup> 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 as 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.<sup>12</sup> 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.<sup>13</sup>

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.<sup>14</sup> 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.<sup>15</sup>

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.

## COMMUNITY DEFENSE TOOLKIT!

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.<sup>1</sup>

**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.<sup>2</sup>

**“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.<sup>3</sup>

**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.<sup>4</sup>

**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.”<sup>5</sup>

**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.

## COMMUNITY DEFENSE TOOLKIT!

# 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.<sup>6</sup> 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.<sup>7</sup> 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.<sup>8</sup>

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.<sup>9</sup> But FCRA does not cover the sale of consumer data for marketing and other purposes—i.e., the business of many data brokers.<sup>10</sup> 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.