DIGITAL ISSUES AWARENESS FOR FRIENDS

LEYM WORKSHOP SERIES

DATA BROKERS & MODERN SURVEILLANCE: DANGERS FOR MARGINALIZED PEOPLE

MARCH 4, 2023

Bill Warters, LEYM Digital Communications Facilitator

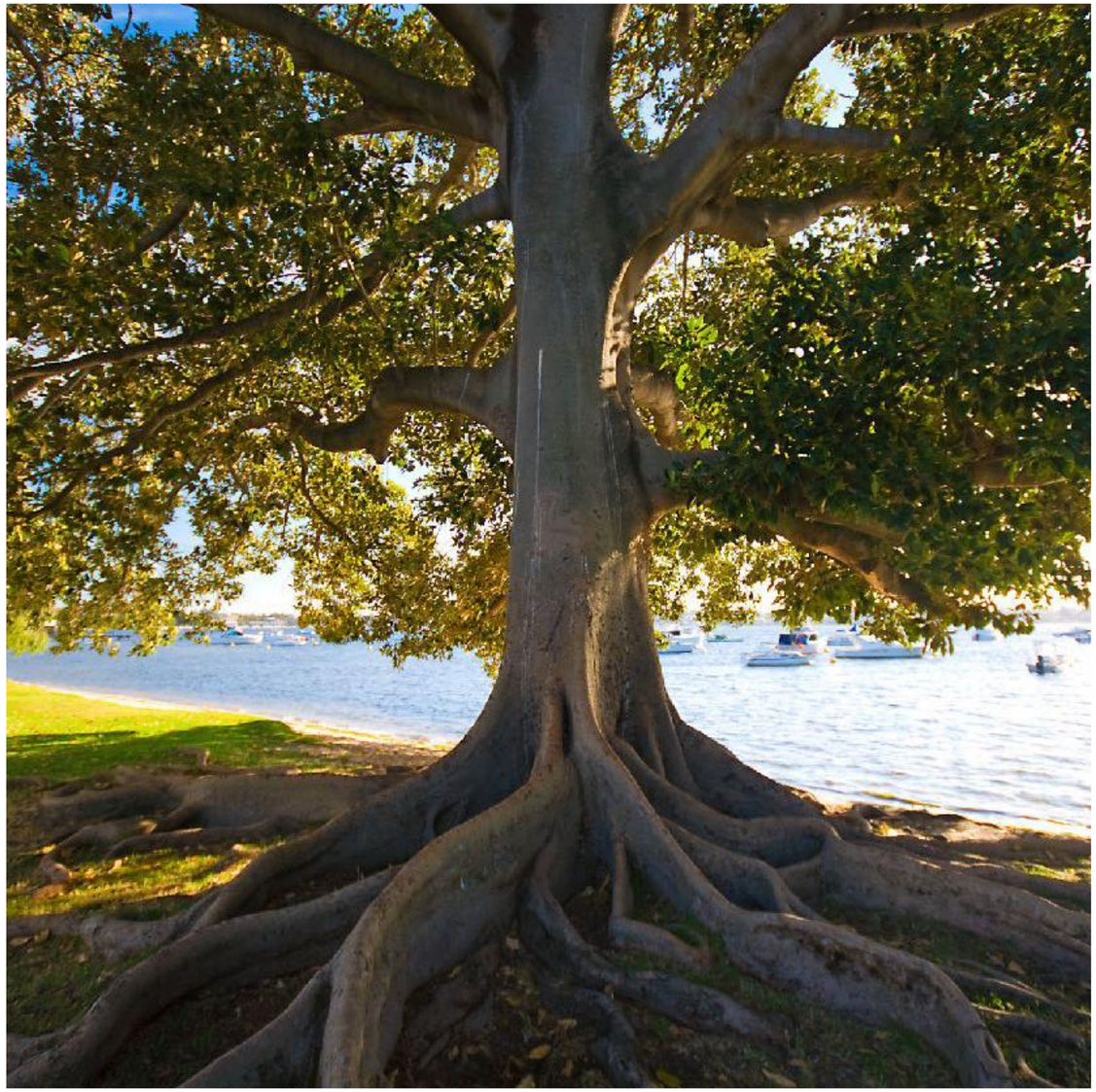
HTTPS://LEYM.ORG/PJE-INTEREST-GROUP/

AGENDA

- Quick Check-in
- Explore DATA Types and Sources
- Review Various Forms of SURVEILLANCE TECHNOLOGY
- Look into the Rise of DATA BROKERS
- Think About"Who's most at Risk?"
- Learn About What's Being Done in Response
- Share Key Resource Links

CHECK-IN

- Name
- Quaker Affiliation
- A Location You are Particularly Fond of



DATA TYPES AND SOURCES

INFORMATION HAS VALUE

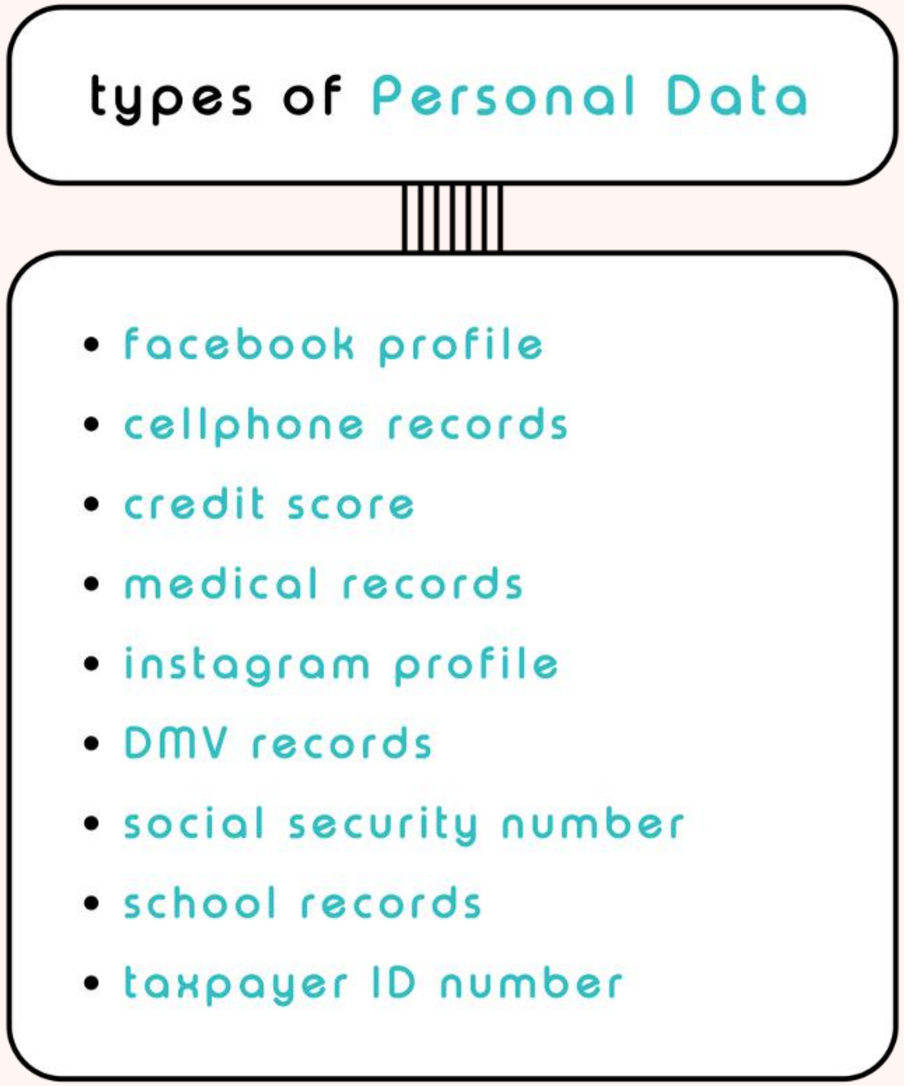
- **What kind of information about us is valuable?**
- **Say, if someone wanted to track you down or learn about your life, how would they do it? What kinds of data would they use?**

DATA is information (facts, interests & behaviors) that technology helps collect and organize.

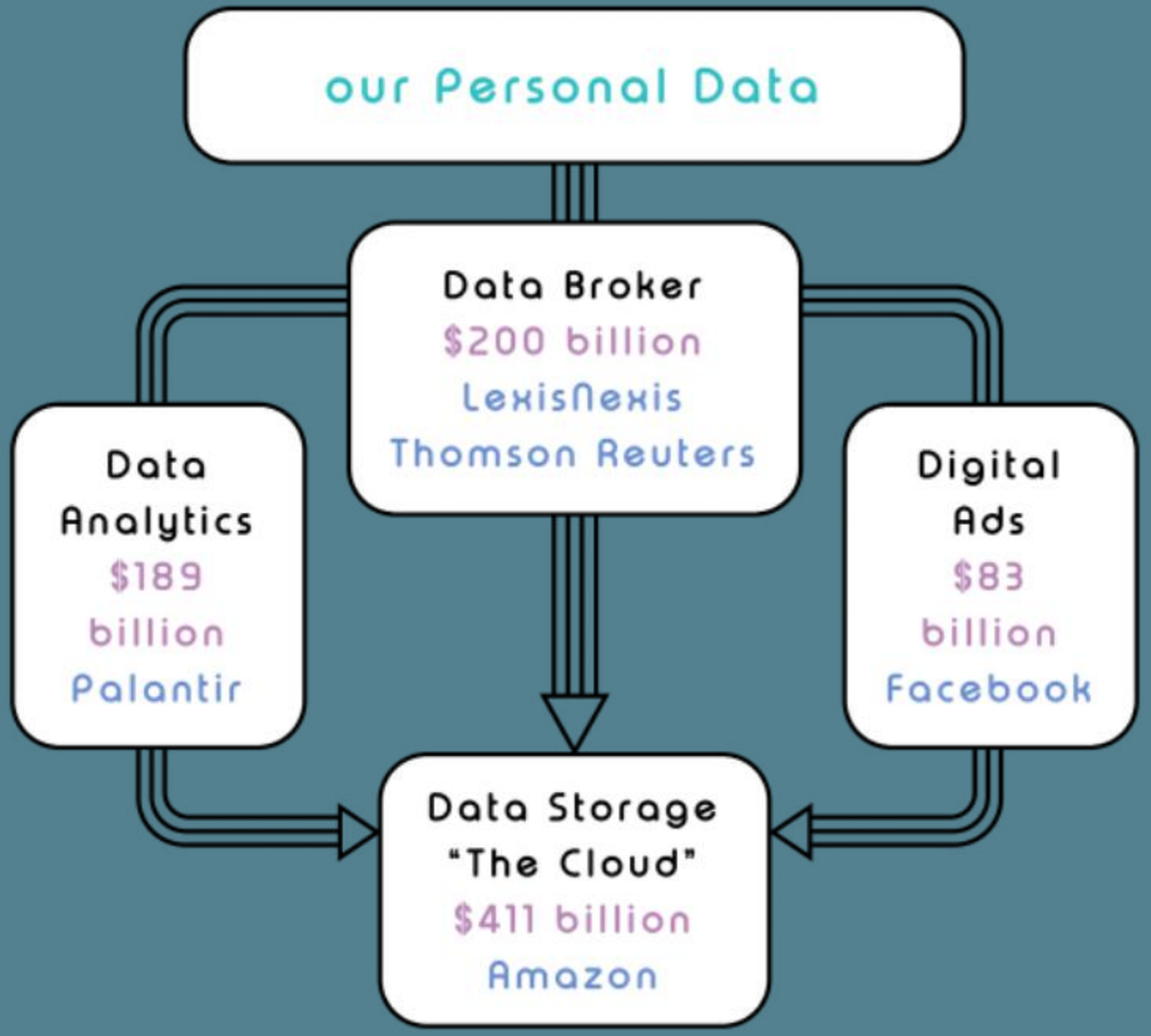
PERSONAL DATA TYPES

- **Personal data is not just the information we enter when we create an account on Facebook or Twitter, but also the types of things we like, do and search on the internet.**

- **<u>Remember</u>: Data is not just facts about us, but also our interests & behaviors online.**



Tech Companies are building wealth with our data through data brokers, data analytics and data storage.



ONLINE ADS & REAL TIME BIDDING

Web-based advertising networks know a LOT about us

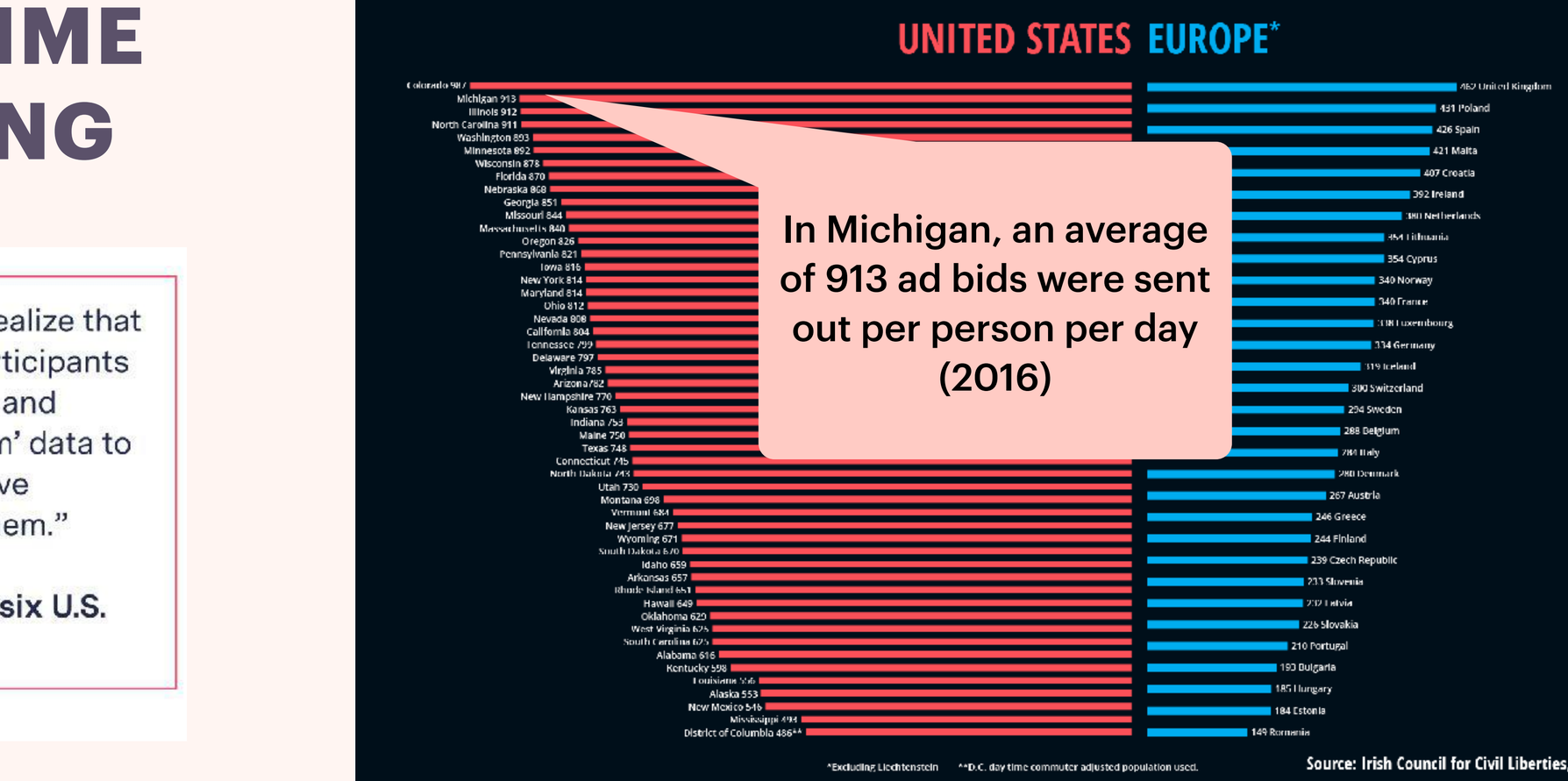
"RTB is also a privacy nightmare. Through RTB, large amounts of personal data exchanges hands between a large number of players a billion times a day. If you're reading an article about erectile dysfunction, depression or self-harm, chances are high, that this will be broadcast to thousands of companies. If you're booking a table, purchased an item at an online retailer, searched for a flight, or read the news, this will also likely be shared with ad exchanges, Supply Side Platforms (SSPs), Demand Side Platforms (DSPs) and countless of other recipients in the ad auction system. **We don't know where our data ends up, we don't know who it is being shared with, and whether it's being used against us in contexts that have nothing to do with advertising.**"

REAL TIME BIDDING

> “Few Americans realize that some auction participants are siphoning off and storing ‘bidstream’ data to compile exhaustive dossiers about them.”
> **Letter to ad tech companies from six U.S. senators**

CORPORATE SURVEILLANCE OF USERS

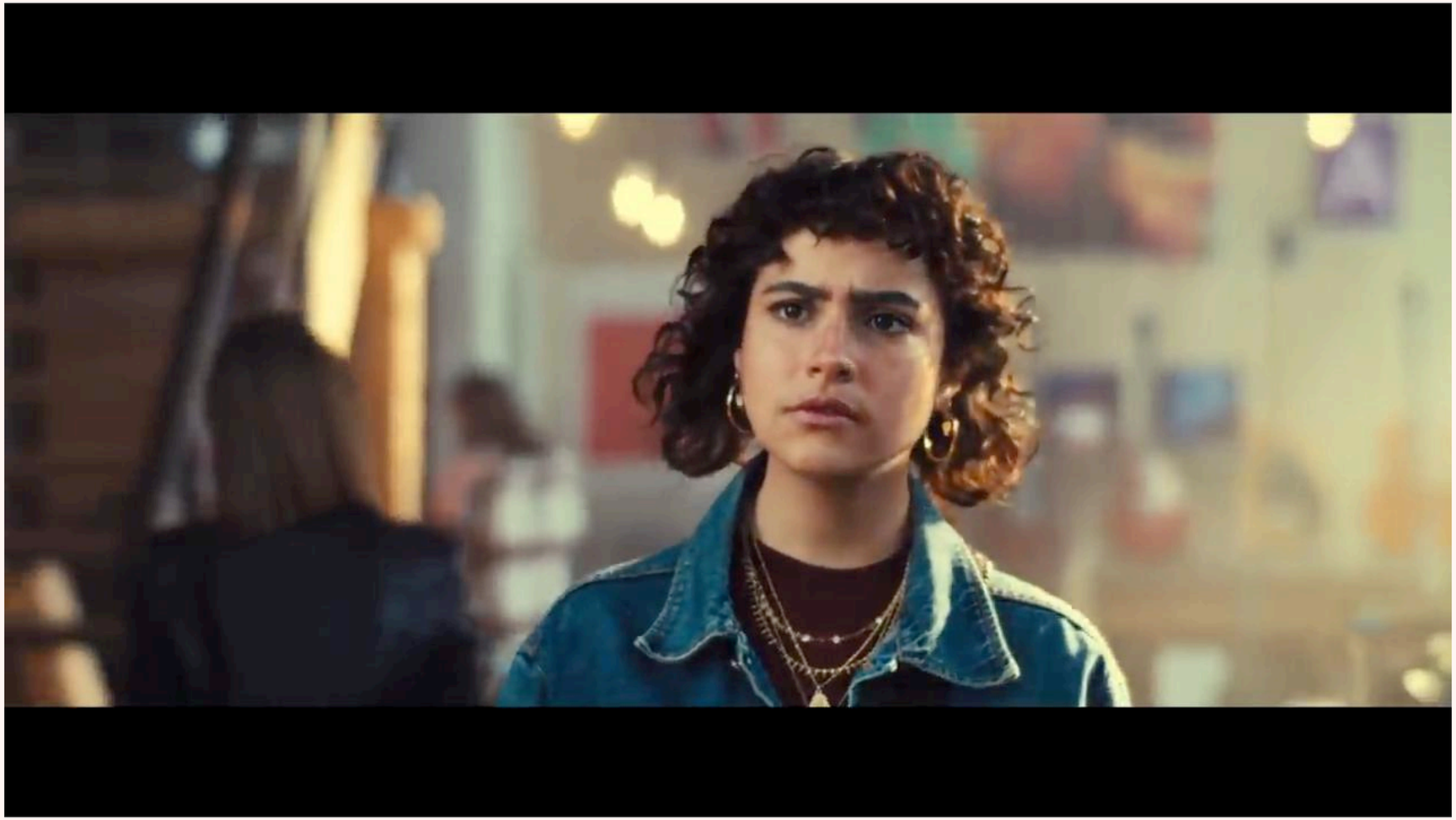
Estimated daily RTB broadcast per person



Real Time Bidding (RTB) is a $117+ billion industry that broadcasts what you are looking at and where you go, no matter how private or sensitive, and broadcasts this data to a host of companies continuously, enabling them to profile you for advertising.

Google is the biggest single company responsible for RTB.

PERSONAL DATA FOR SALE



See this Apple Ad on Privacy at https://www.youtube.com/watch?v=NOXK4EVFmJY

SUPERMARKET SHOPPING DATA

- The Markup took a deep dive into Kroger's use of customer data.
- Kroger: "We have collected over 2,000 variables on customers"
- Tracking 2 billion annual transactions across 60 million households with a persistent household identifier
- Information they say they may collect and use
  - ☑ Personal Information
  - ☑ Purchase History (going back up to 18 years)
  - ☑ Location (even in-store via Kroger app)
  - ☑ Financial and Payment info
  - ☑ Health-related info
  - ☑ Mobile device data
  - ☑ Demographic data
  - ☑ Biometric data
    (in-store facial recognition with warning signs)
  - ☑ Behavioral inferences

Privacy

Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You

When you use supermarket discount cards, you are sharing much more than what is in your cart—and grocery chains like Kroger are reaping huge profits selling this data to brands and advertisers

By Jon Keegan

February 16, 2023 08:00 ET

https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you

LOCATION DATA FROM CARS

- **The Markup identified 37 companies that are part of the connected vehicle data industry**
- **One data hub called Wejo claims its data represents “one in every 28 vehicles in the USA” with 16.2 trillion data points and 76.7 billion journeys with accuracy down to 3 meters.**
- **Wejo’s investors include GM, Microsoft and defense and intelligence contractor Palantir.**

“Vehicle data hubs ingest vehicle and movement data from multiple sources: from car manufacturers, other connected vehicle data providers, directly from vehicles using aftermarket hardware such as “onboard diagnostics” (OBD) dongles, or from smartphone apps. The data is then consolidated and normalized in one place for analysis and insights.”

The Breakdown

Who Is Collecting Data from Your Car?

A firehose of sensitive data from your vehicle is flowing to a group of companies you’ve probably never heard of

By Jon Keegan and Alfred Ng

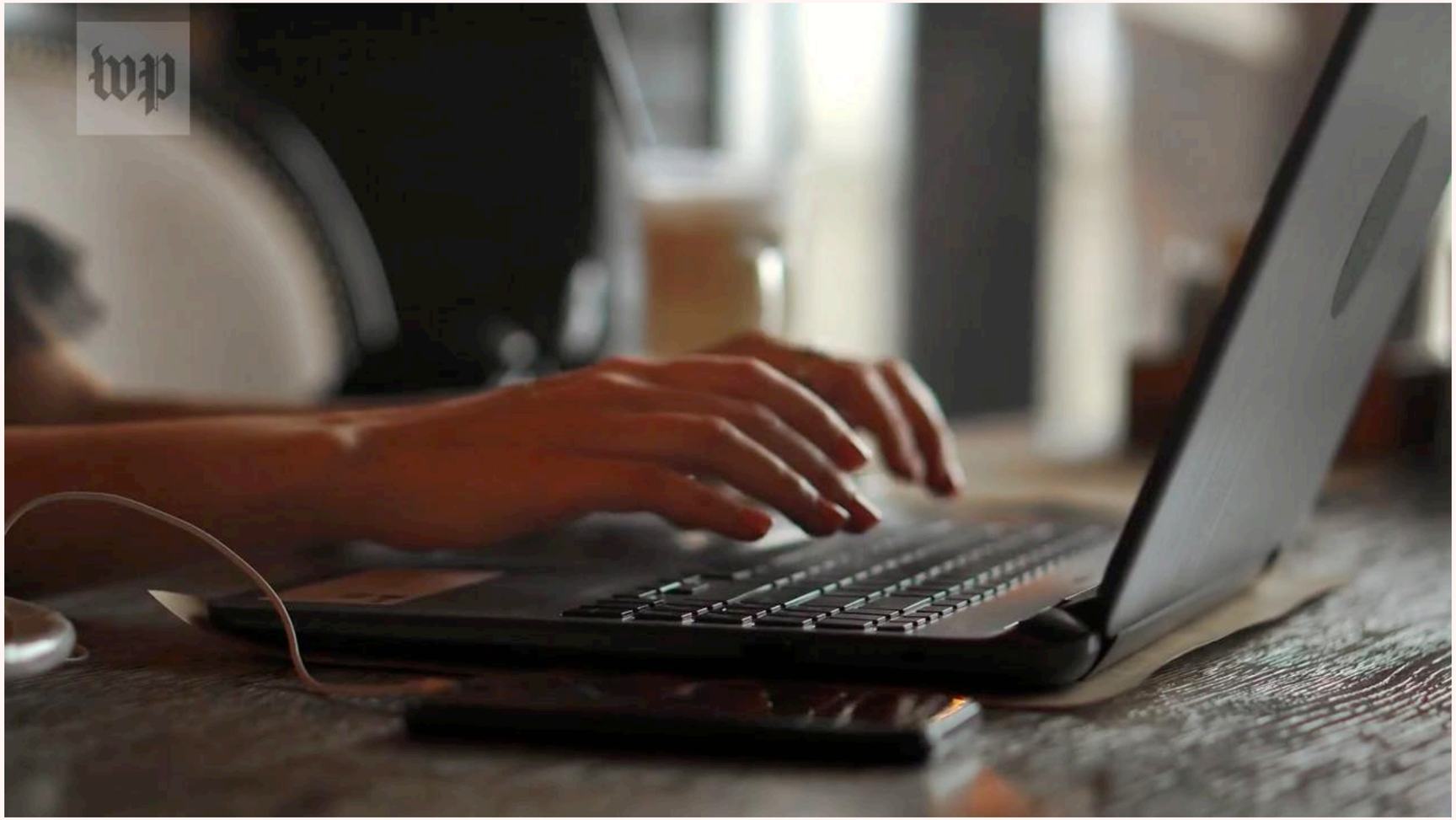
July 27, 2022 08:00 ET

Ryan Raphael

https://themarkup.org/the-breakdown/2022/07/27/who-is-collecting-data-from-your-car

SURVEILLANCE TECHNOLOGY

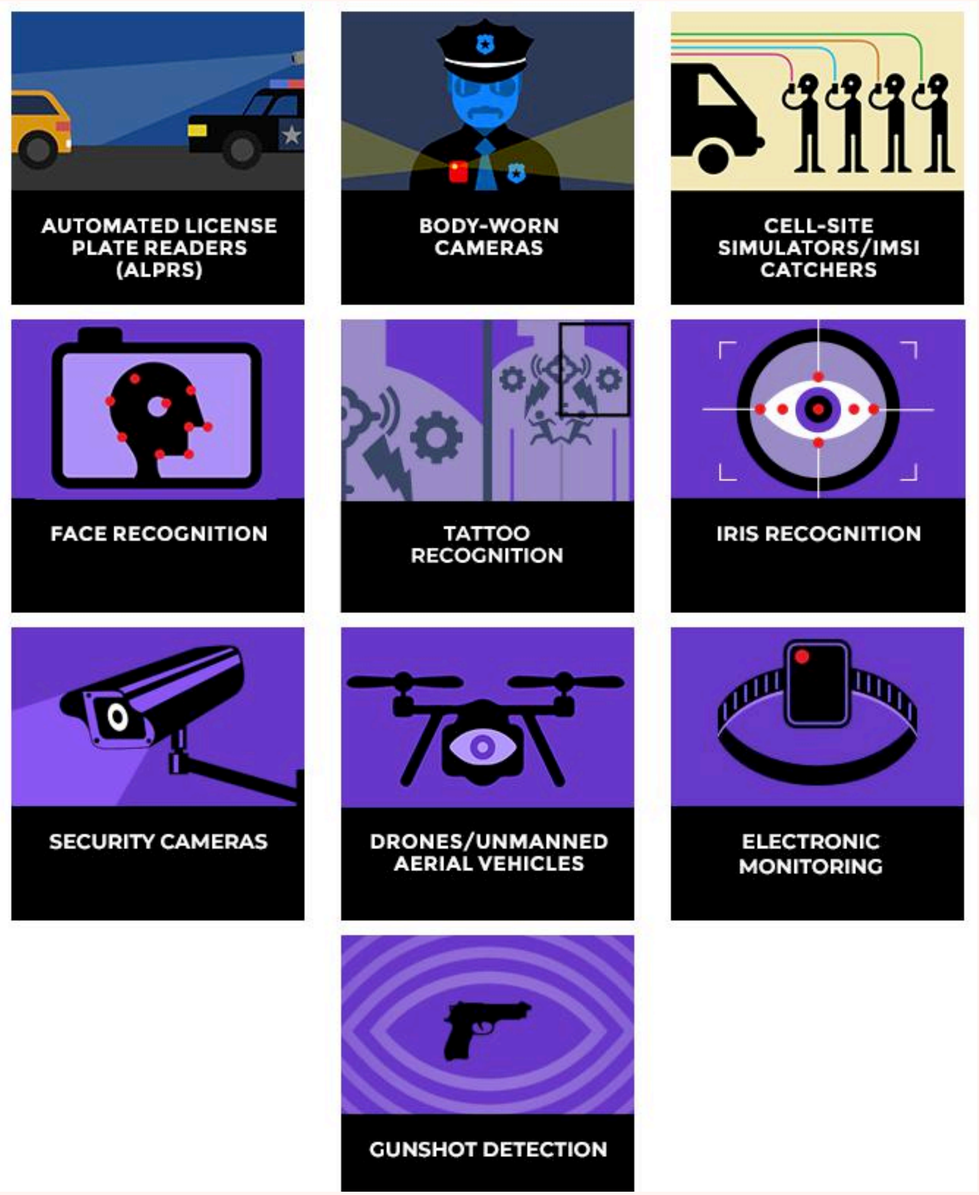
SURVEILLING THOSE WORKING REMOTELY



https://www.youtube.com/watch?v=zg0MC2pEuYY

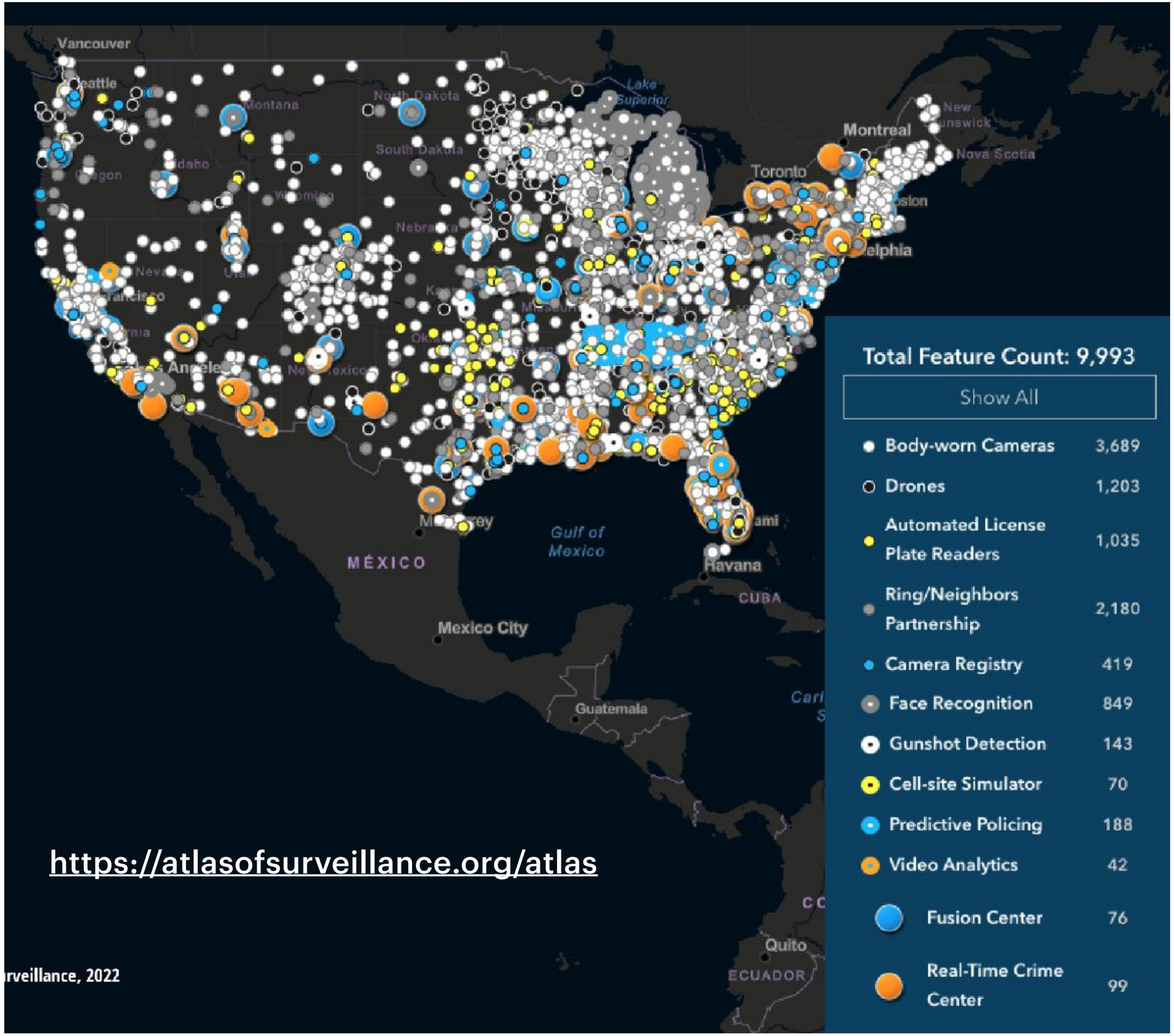
SURVEILLANCE TECH IN OUR CITIES

- **Cities are increasingly monitored using a wide range of technologies**
- **The EFF has created materials explaining how each of the technologies works & how it is being used & abused**
- **Protesters & undocumented people are often targeted**



See overview and learning materials here: https://www.eff.org/issues/street-level-surveillance

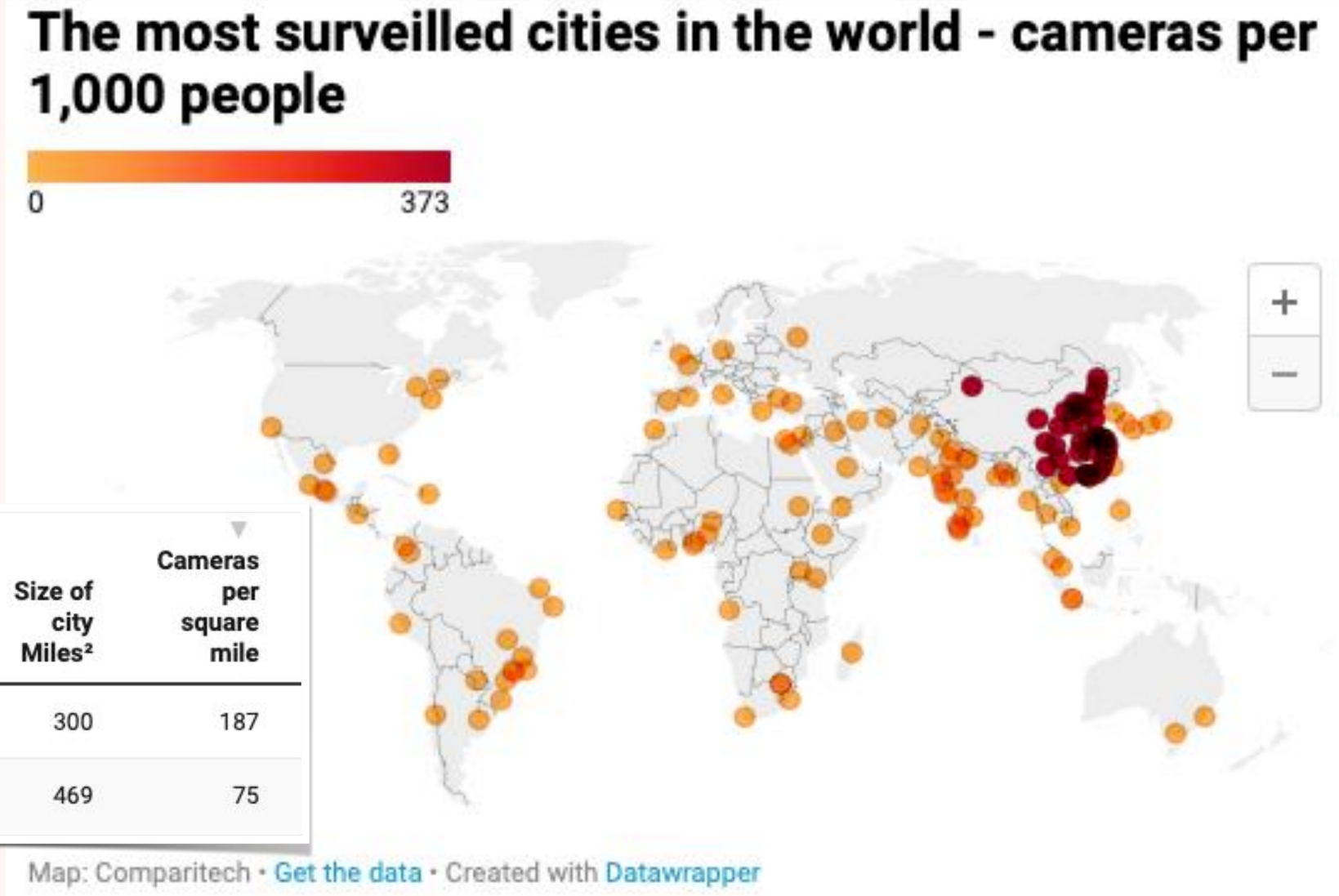
PUBLIC SURVEILLANCE MAPPED



https://atlasofsurveillance.org/atlas

rveillance, 2022

CCTV CAMERAS USED GLOBALLY

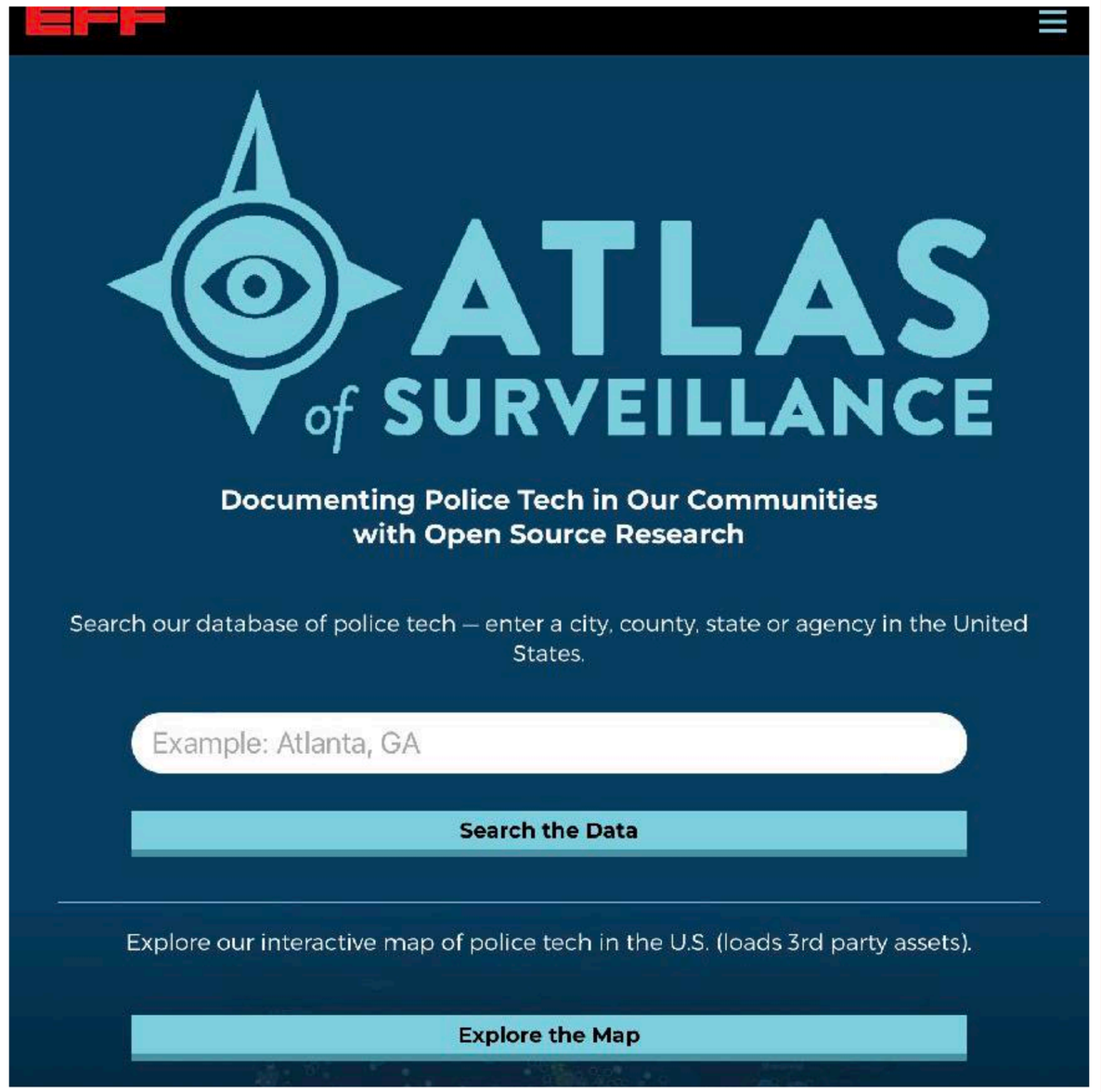


City	# of CCTV Cameras	# of People (2022)	# of CCTV Cameras per 1,000 People	Size of city Miles²	Cameras per square mile
New York	56,190	8.18M	6.87	300	187
Los Angeles	34,959	3.99M	8.77	469	75

https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

EXAMPLES OF POLICING TECHNOLOGY

- **The Electronic Frontier Foundation (EFF) has done research on what kinds of surveillance tech is being used across the United States**
- **Let's try doing a search for cities we care about**
- **https://atlasofsurveillance.org**

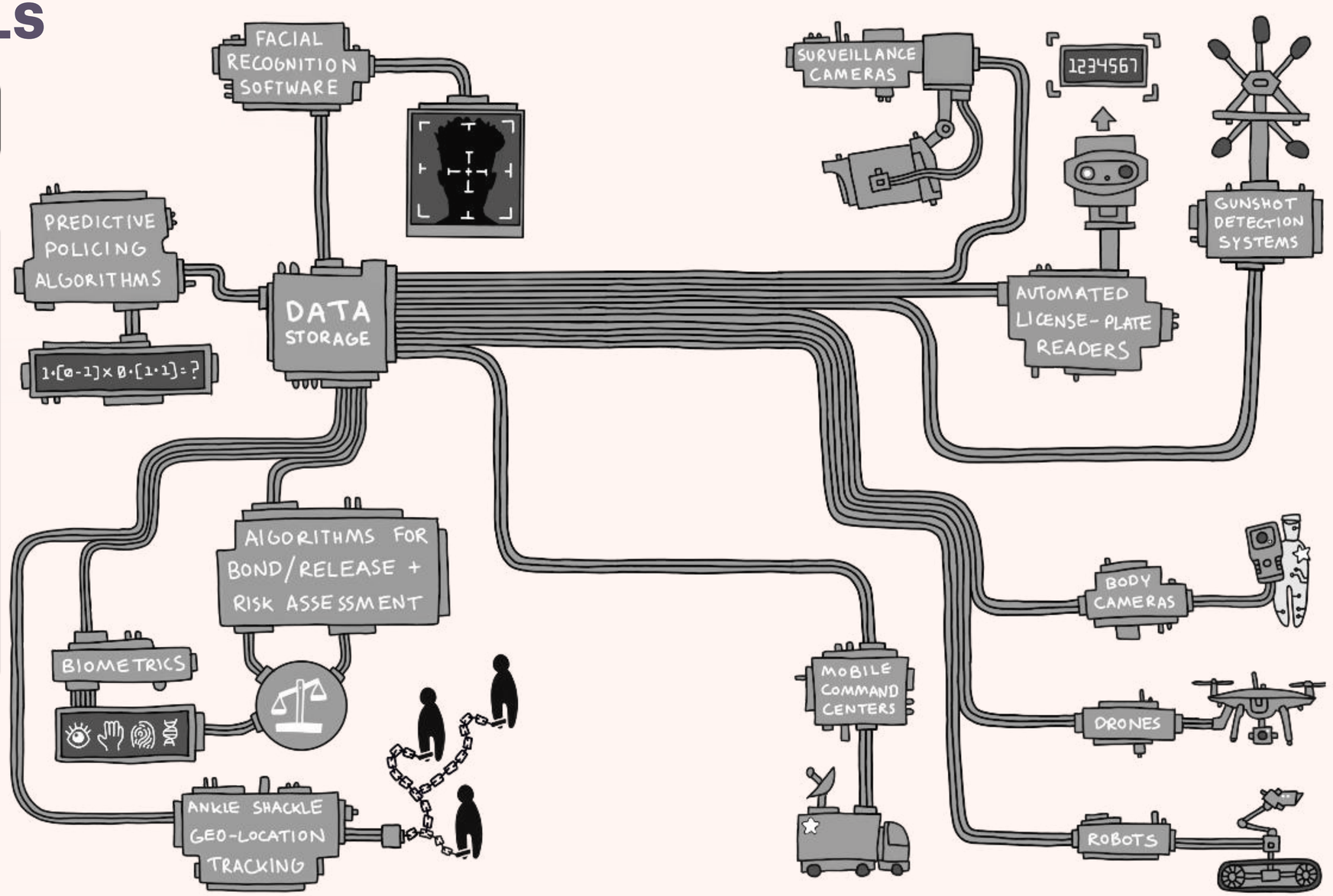


JUSTICE SYSTEM TOOLS

Tech Tools Used by Police & Justice System

- Facial Recognition Software
- Surveillance Cameras
- Gunshot Detection Systems
- Automated License Plate Readers (ALPR)
- Body Cameras
- Drones
- Robots
- Biometrics
- Ankle Shackles/Geo Location Tracking
- Algorithms for Bonds/Release & Risk Assessment
- Predictive Policing Databases

BRAINSTORM: Ways in which the technologies in this chart harm communities.



REPORT ON 21ST CENTURY POLICING

The RISE and REACH of Surveillance Technology

"Adopted for use as police "reforms," sophisticated electronics and tech capabilities do not address the unchecked power and ballooning budgets of local police departments. Instead, they open the door for law enforcement to monitor communities while private companies profit from sales and contracts. As the movement to defund the police becomes impossible to ignore, replacing police officers with police cameras is called progress"

https://acrecampaigns.org/research_post/21st-century-policing/

ELECTRONIC MONITORING

Today, authorities primarily apply electronic monitors to four populations:

People on pretrial release.

Individuals who have completed a prison or jail sentence and have EM as a condition of their parole or probation.

Immigrants under the authority of Immigration and Customs Enforcement (ICE).

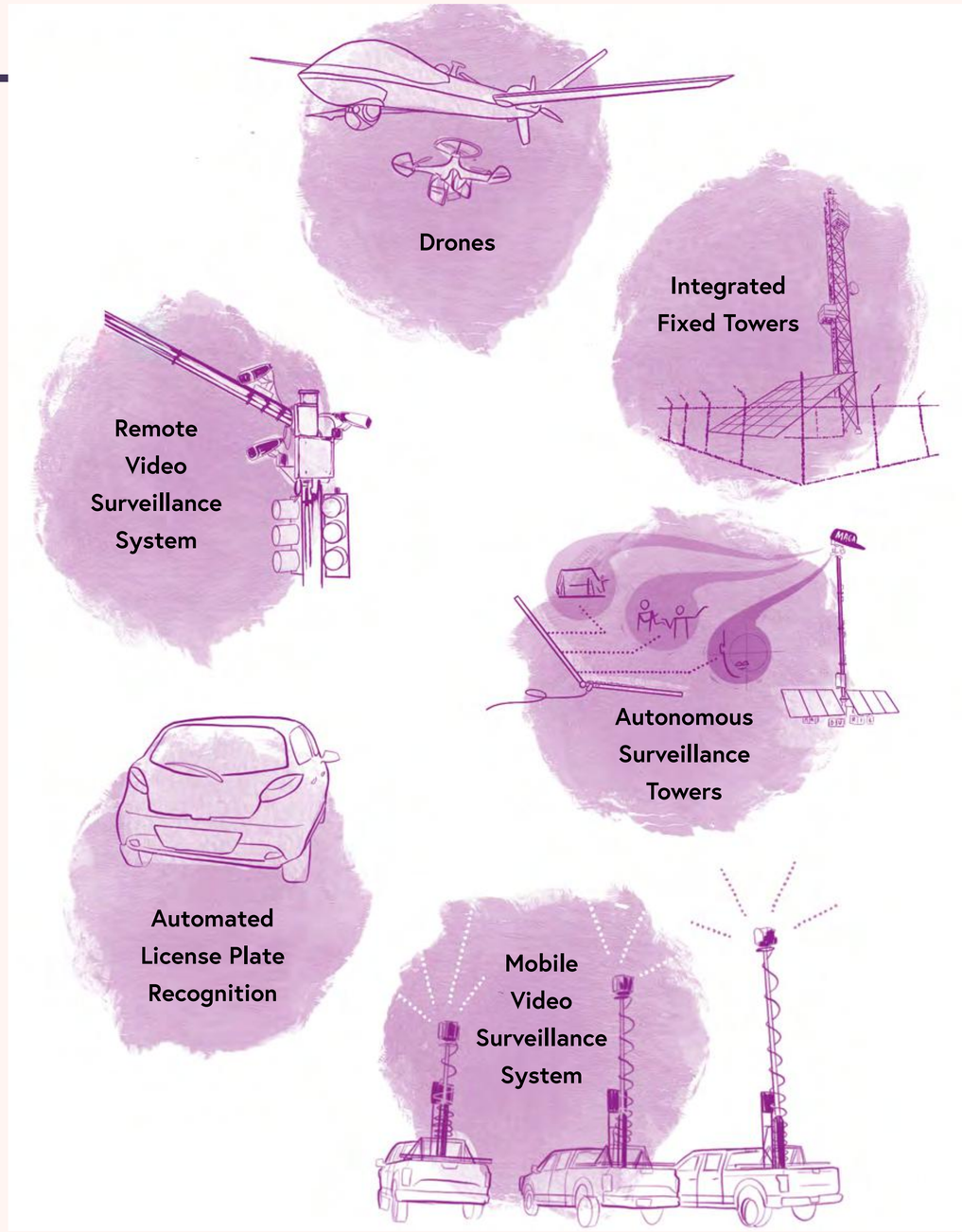
Youth under the supervision of the juvenile court.

EM widens the net of incarceration. Monitoring is making homes into jail cells and turning Black and brown communities into open-air prisons, continuing the punishment and mass incarceration process that has been going on for decades, in some cases for centuries.

https://mediajustice.org/unshackling-freedom/what-you-should-know/

BORDER TECHNOLOGY

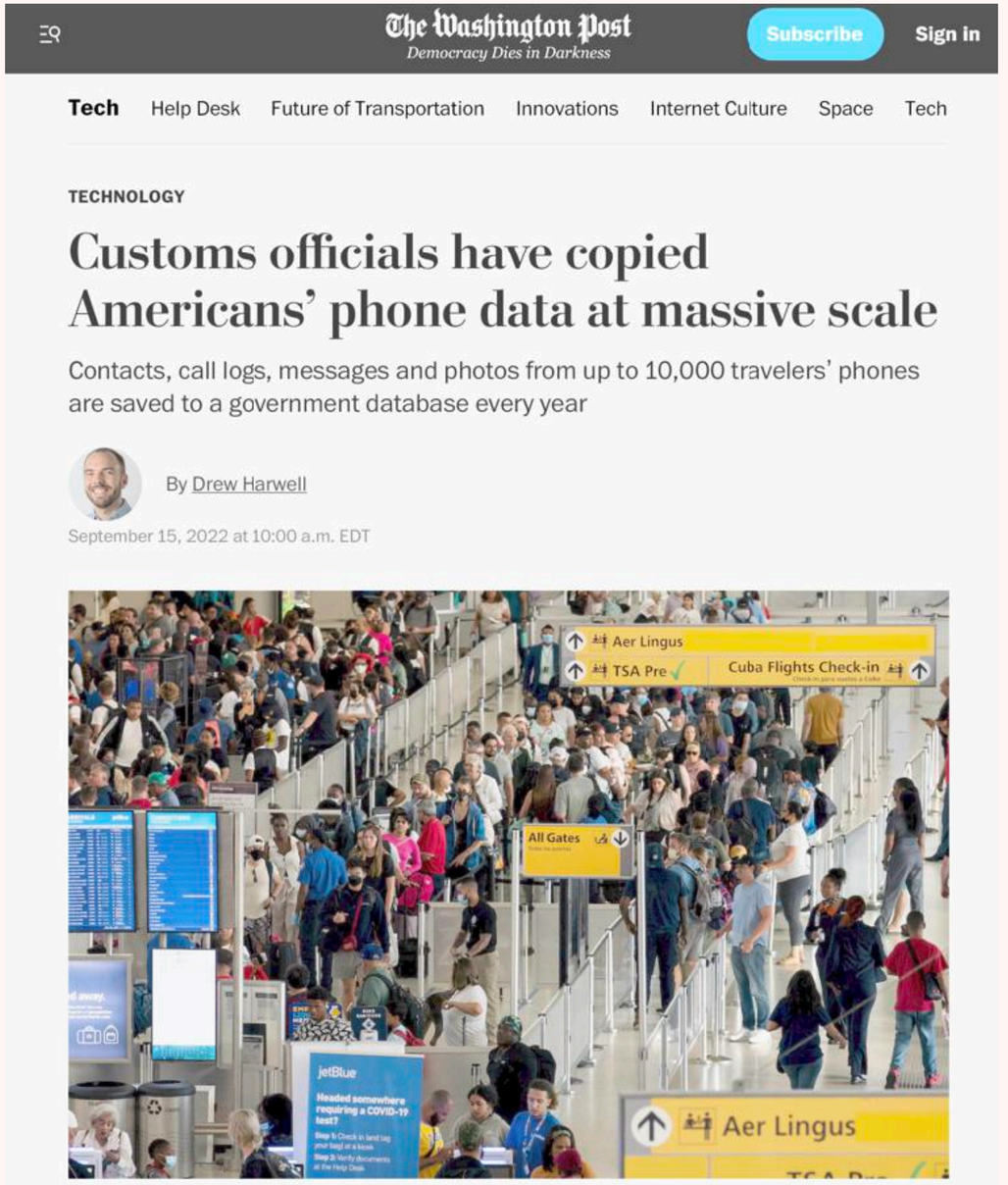
- **Mijente, Just Futures Law & the No Border Wall Coalition produced a comprehensive report on the ever-expanding set of digital tools used to surveil our borders**
- **The Deadly Digital Border Wall report is available here.**
- **The report covers the "digital wall" of surveillance towers, drones, cameras, and license plate readers as well as biometrics in use such as DNA, facial recognition, voice recognition and iris scans, AND the hacking of phones and vehicle information systems to gather personal data**
- **Roughly two-thirds of the U.S. population lives within the 100-mile "border zone" defined by CBP, including nine out of the 10 largest cities.**
- **EFF has worked with reporters to create reports on tech used in key Southwestern Border Communities here: https://www.eff.org/pages/atlas-surveillance-us-mexico-border-communities**



Deadly Digital Border Wall report: https://notechforice.com/wp-content/uploads/2021/10/Deadly.Digital.Border.Wall_.pdf

CELL PHONE PRIVACY RIGHTS WAIVED WITHIN 100 MILES OF US BORDERS

- **Reports show that Customs officials have copied contacts, call logs, messages and photos from up to 10,000 travelers' phones yearly**
- **This data is saved to government databases**
- **In 2021 a federal appeals court ruled that CBP does not need a warrant to search people's mobile devices who are entering the country, whether or not they are U.S. citizens. Agents have the legal authority to go through any device within 100 miles of the border and to take devices away from travelers for up to five days without providing justification.**



The Washington Post
Democracy Dies in Darkness

Subscribe Sign in

Tech Help Desk Future of Transportation Innovations Internet Culture Space Tech

TECHNOLOGY

Customs officials have copied Americans' phone data at massive scale

Contacts, call logs, messages and photos from up to 10,000 travelers' phones are saved to a government database every year

By Drew Harwell

September 15, 2022 at 10:00 a.m. EDT

https://www.reuters.com/article/us-usa-immigration-privacy/u-s-border-agents-do-not-need-warrants-to-search-digital-devices-court-rules-idUSKBN2AA2AL

https://www.washingtonpost.com/technology/2022/09/15/government-surveillance-database-dhs/

THE RISE OF DATA BROKERS

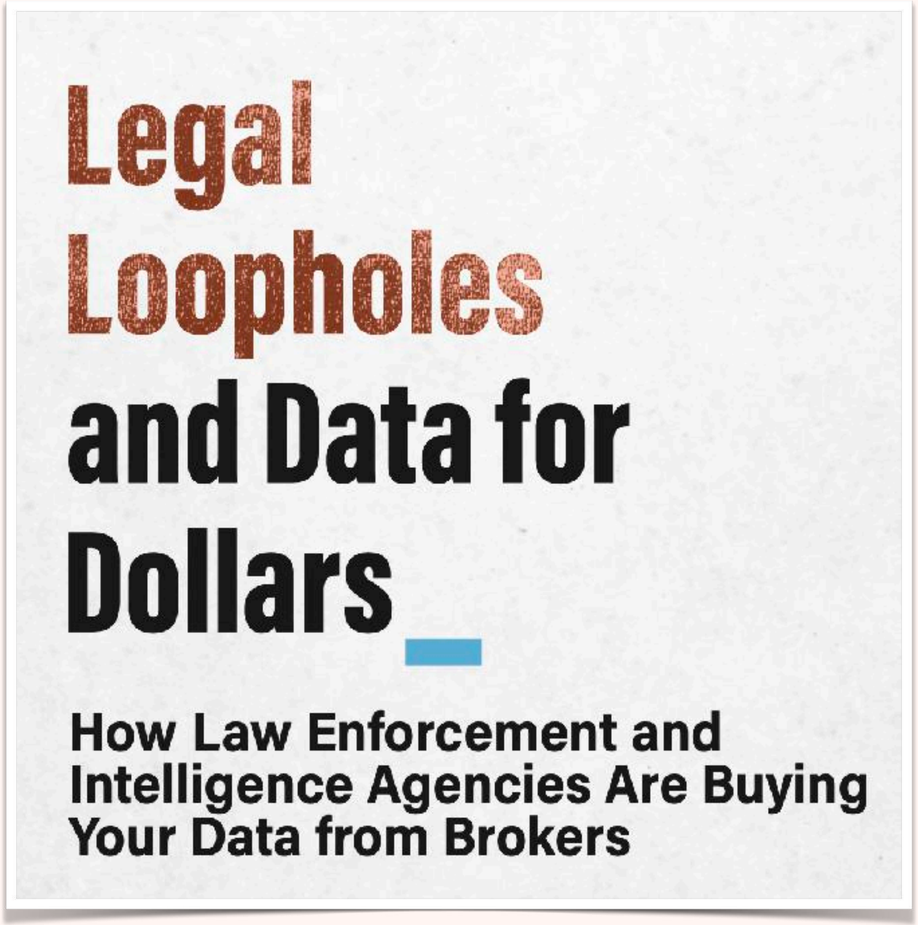
COMMERCIAL DATA SOURCES USED FOR FEDERAL SURVEILLANCE

https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600

DATA BROKERS AND GOVERNMENT AGENCIES

- **Your profile is for sale, and it gets more detailed over time**
- **Legal privacy protections may be side-stepped by using commercial services**

"The problem is a byproduct of the lucrative private market for personal data, where many companies that offer online services collect, analyze, and sell data about individuals using those services. This **data is aggregated by companies called 'data brokers'** that typically lack any direct relationship with the individuals whose data they collect and sell, but may accumulate personal data from multiple sources with varying degrees of granularity, ranging from anonymized trends to the specific locations of individuals at specific times. Advertisers, retailers, and other companies may then seek access to data for varied commercial purposes."



Center for Democracy & Technology. Report by Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim and Dhanaraj Thakur

https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/

LEXISNEXIS AS A DATA BROKER

Vast Repository

of Public and Commercially Available Data

- Insurance Records
- Consumer Records
- Unique Name/Address Combinations
- Property Records
- Motor Vehicle Records
- Bankruptcy Records Monitored
- Vehicle Title Records
- Unique Cell Phones
- Unique Person Identities
- Active U.S. Business Entities

LEXISNEXIS VIRTUAL CRIME CENTER

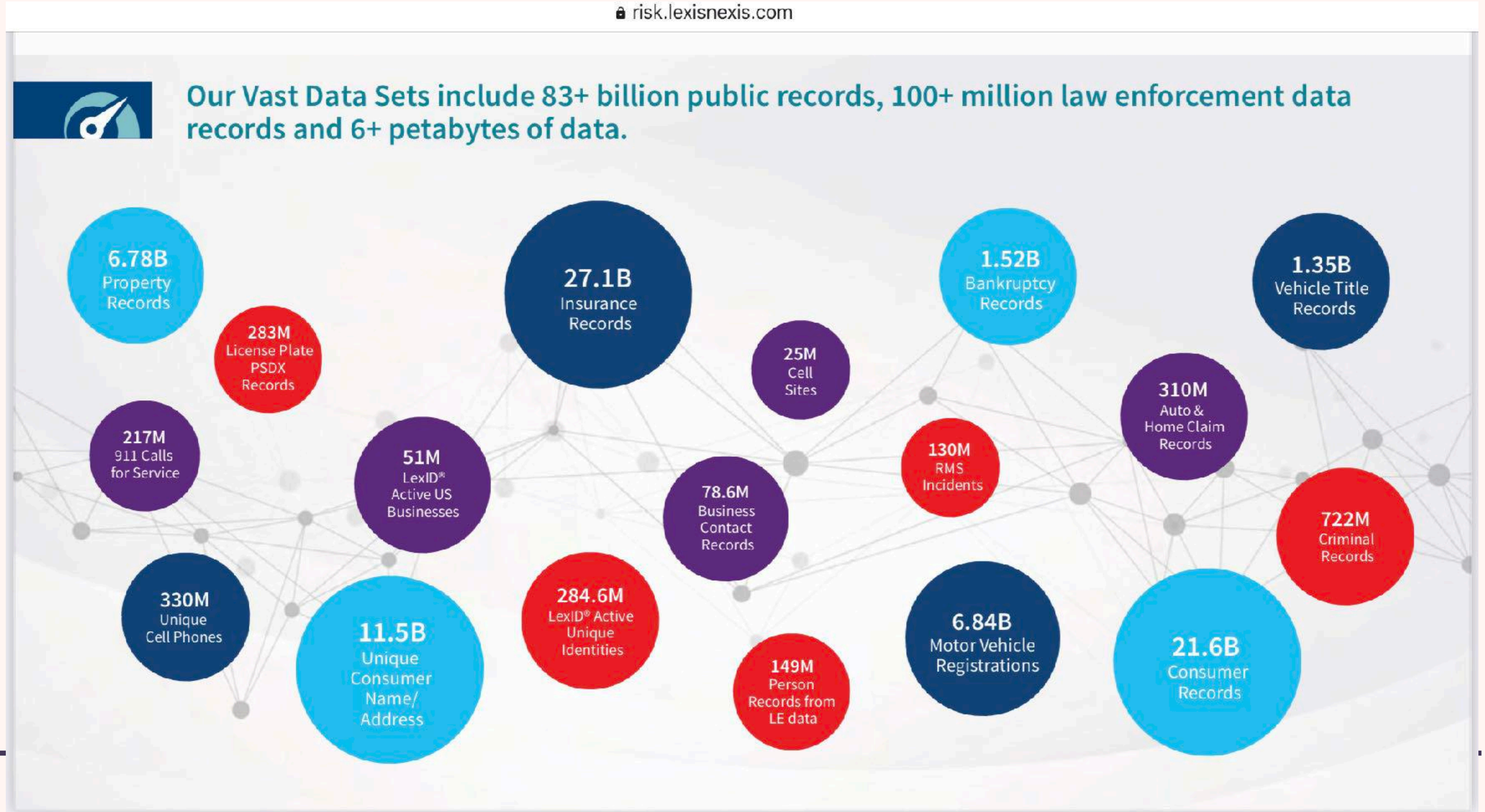
“Today’s law enforcement agencies need a view beyond their own jurisdictions. **LexisNexis Accurint Virtual Crime Center brings together disconnected data from over 10,000 different sources**, including police agencies nationwide and public records for intelligence-led policing that can then drive decisions and actions,” the website for the Virtual Crime Center reads.”

“Zach Edwards, a security researcher who follows the data trading ecosystem, told Motherboard in an online chat that “‘**relatives, neighbors & associates information**’ is totally alarming. It would appear that LexisNexis has taken the concept of ‘friends and family plans’ to a whole new creepy level, by creating consumer profiles available for purchase to the government, with details about people's close personal contacts.””

☑ **Contains dossiers on roughly two-thirds of the US population**

https://www.vice.com/en/article/y3p8j5/lexisnexis-selling-data-government

LEXISNEXIS' VAST DATA SETS



FOG DATA SCIENCE

- Data broker gathers data from apps people use all the time. Pays developers to pass it on to them.
- Claims to have “billions” of data points about “over 250 million” devices and that its data can be used to learn about where its subjects work, live, and associate.
- Fog states that it has access to a “near real-time” database of billions of geolocation signals derived from smartphones.
- Can access historical data going back to 2017
- Provides both “Area Searches” and “Device Searches”

Fog’s service is especially dangerous in the wake of the Supreme Court’s Dobbs decision. Many states have criminalized abortion, giving state & local police license to unleash their surveillance powers against people seeking reproductive healthcare as well as the professionals that provide it. Fog Reveal lets an officer sitting at a desk **draw geofences around abortion clinics anywhere in the world, then track all devices seen visiting them**.

https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police

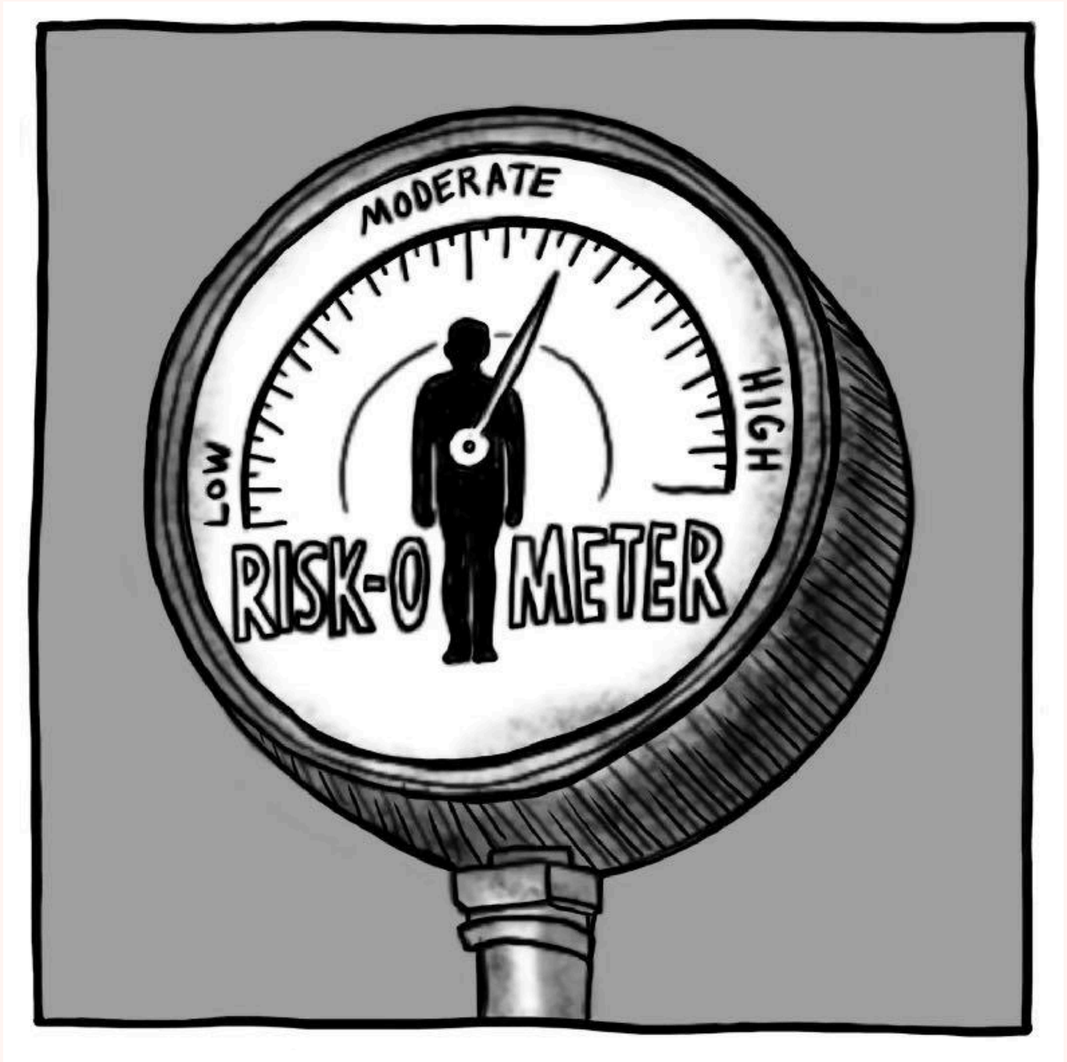
THOMSON REUTERS CORP

- Thomson Reuters provides access to massive databases of personal information to U.S. Departments of Justice (DOJ) and Homeland Security (DHS). From 2007 to 2021, the company was directly awarded more than 7,500 U.S. federal contracts worth at least $1.5 billion.
- Flagship product is called CLEAR (Consolidated Lead Evaluation and Reporting)
- CLEAR provides DMV records, real estate ownership, utilities data, professional licenses, criminal and court records, healthcare provider content, consumer and credit bureau data, real-time incarceration and arrest records, business data, data from social media platforms, chatrooms, and blogs, and live access to over 7 billion license plate detections.

WHO IS MOST AT RISK?

VULNERABLE GROUPS

- ☑ People of color and religious minorities
- ☑ Immigrants
- ☑ Undocumented people
- ☑ Protestors and Activists
- ☑ People caught up in the criminal justice system
- ☑ People seeking reproductive health services
- ☑ Unhoused people
- ☑ LBGTQ+ people
- ☑ People with Disabilities



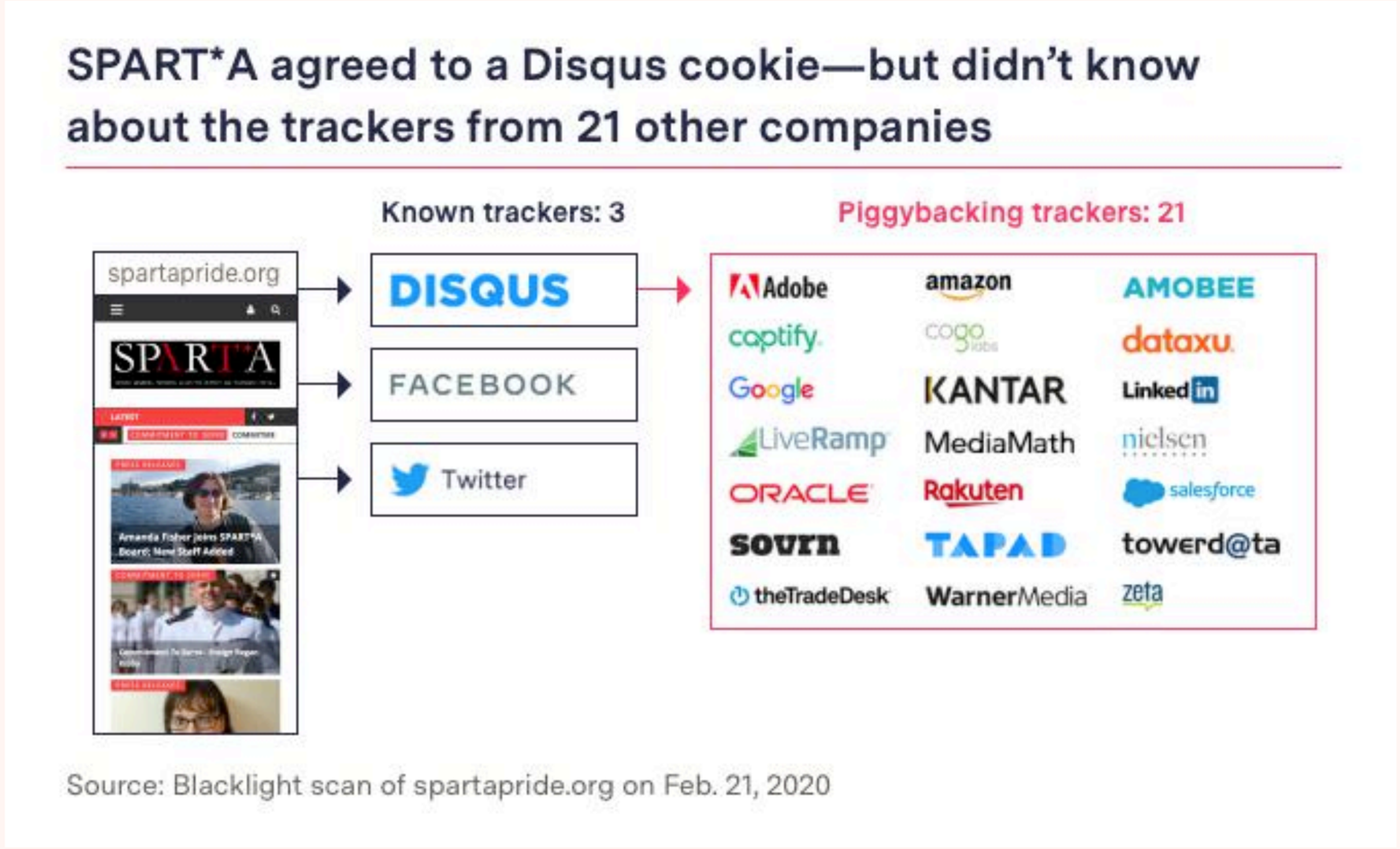
EMBEDDED WEBSITE TRACKERS ARE A BIGGER PROBLEM THAN MOST WEBSITE HOSTS EVEN REALIZE

- ☑ **More than 100 websites serving undocumented immigrants, domestic and sexual abuse survivors, sex workers, and LGBTQ people sent data about their visitors to advertising companies.**
- ☑ **Eighty U.S. abortion providers loaded third-party trackers on user browsers, some of them sending data to Facebook that ended up in user profiles.**
- ☑ **Trackers from different companies were communicating with each other to confirm the identity of visitors to a website for victims of sexual violence.**
- ☑ **Health information websites like Everyday Health and WebMD sent user data about page visits to dozens of marketing companies.**
- ☑ **The Arizona Department of Child Safety's page on how to report child abuse sent data about site visitors to six ad tech companies.**

"In other words, website operators are often effectively as blind to exactly what information advertising companies and marketers are collecting from their website visitors—and what they're doing with the data—as the people browsing the internet are."

https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites

Tracking Cookies Example:
Spart*a is a small nonprofit serving **transgender military service members and veterans**



Privacy

Gay/Bi Dating App, Muslim Prayer Apps Sold Data on People's Location to a Controversial Data Broker

The Markup identified 107 apps that sold data to X-Mode in 2018 and 2019

January 27, 2022 08:00 ET

https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites

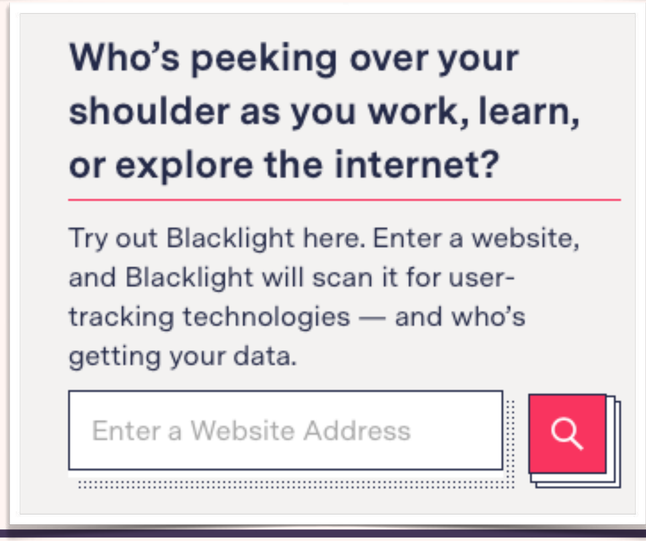
BLACKLIGHT WEBSITE PRIVACY CHECKER

The types of surveillance that Blacklight seeks to identify are:

- ☑ **Third-party cookies**
- ☑ **Ad trackers**
- ☑ **Key logging**
- ☑ **Session recording**
- ☑ **Canvas fingerprinting**
- ☑ **Facebook tracking**
- ☑ **Google Analytics “Remarketing Audiences”**

Go to this website to run a test:
https://themarkup.org/blacklight

> “I like to think of Blacklight as a meat thermometer that you can stick into any website and get an instant reading on its level of creepiness.”



SURVEILLANCE OF REPRODUCTIVE HEALTH

- **Period Tracking Apps, Car License Plate Data and Pregnancy Registers are all being weaponized to monitor women**
- **Surveillance data and technology are being exploited to stoke fear and prevent abortions in countries including the United States, China, Hungary and Poland**
- **Tactical Tech reviews the landscape in their piece "Cycles of Control: Private Companies and the Surveillance of Reproductive Health"**

Abortion surveillance: How women's bodies are being monitored

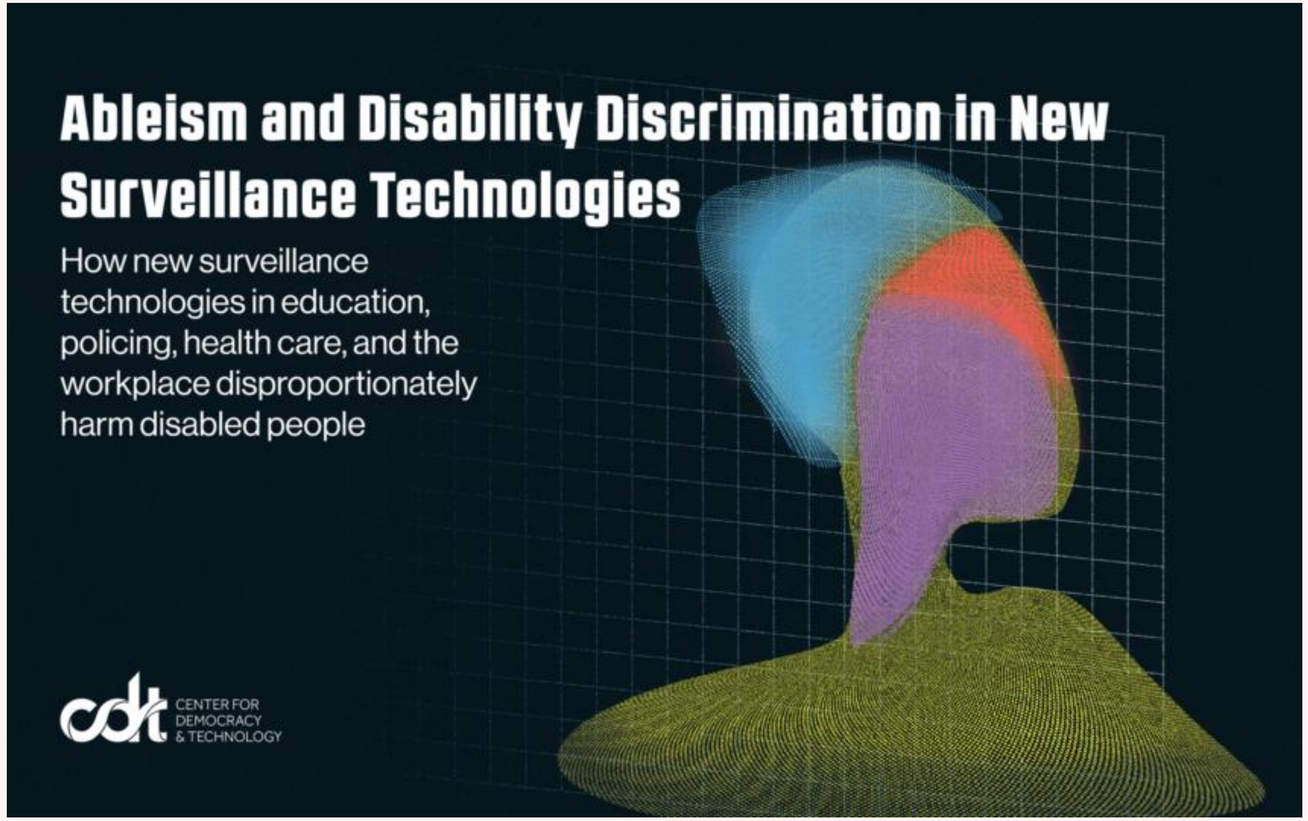
Period tracking apps, car licence plate data and pregnancy registers are the latest tools experts warn are being harnessed to monitor women

By Harriet Barber, GLOBAL HEALTH REPORTER
10 October 2022 • 9:37am

https://www.telegraph.co.uk/global-health/women-and-girls/new-abortion-surveillance-state-keeping-tabs-women/

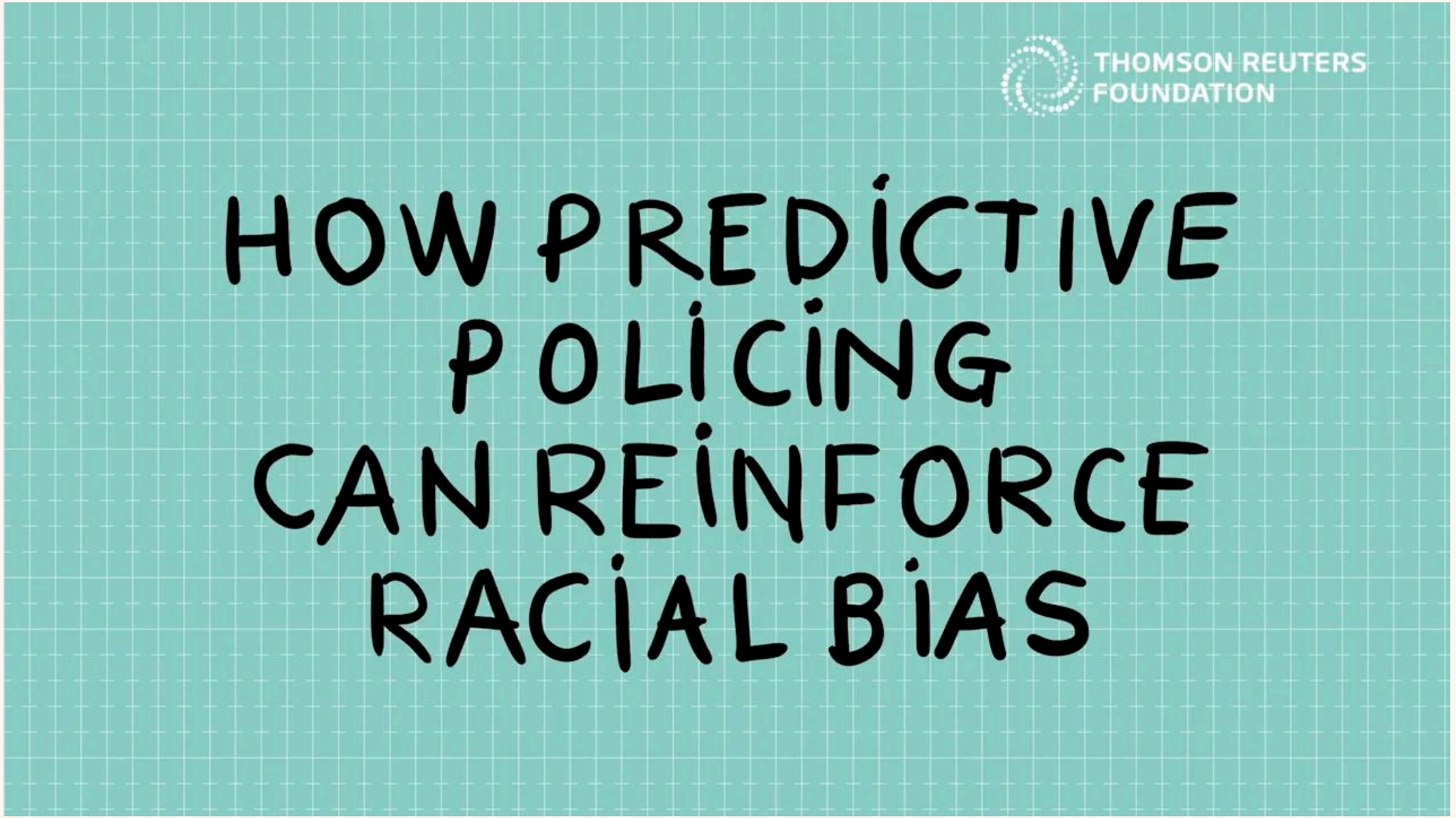
DISABILITY DISCRIMINATION IN NEW SURVEILLANCE TECHNOLOGIES

- **This report from the Center for Democracy and Technology examines four areas where algorithmic and/or surveillance technologies are used to surveil, control, discipline, and punish people, with particularly harmful impacts on disabled people.**
- **(1) Education**
- **(2) the Criminal Legal System**
- **(3) Health Care**
- **(4) the Workplace**



https://cdt.org/insights/ableism-and-disability-discrimination-in-new-surveillance-technologies-how-new-surveillance-technologies-in-education-policing-health-care-and-the-workplace-disproportionately-harm-disabled-people/

PREDICTIVE POLICING AND RACIAL BIAS



https://www.youtube.com/watch?v=ZU_o87c08l4

DETROIT REAL-TIME CRIME CENTER

- ☑ As of March 2019, the RTCC has access to more than 6000 live video feeds
- ☑ Automated License Plate Readers track vehicle movements
- ☑ 787 Smart Traffic Lights, many with live cameras
- ☑ Contracts for Facial Recognition and Command Central Aware crime analysis software suites
- ☑ Creation of Neighborhood Real-Time Intelligence Program using $9 million of local and federal traffic modernization funds to put up 500 new high definition cameras

Detroit Real-Time Crime Center

Detroit Police Department
Detroit, Michigan

Source: Detroit Police Department

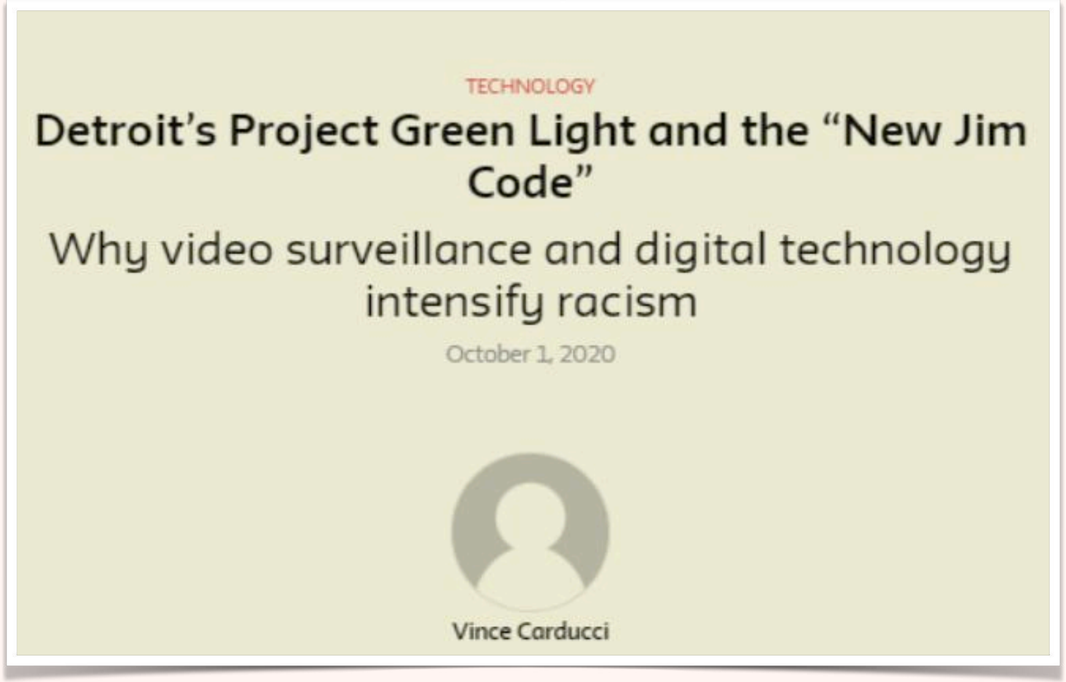
See Info on Detroit Real-Time Crime Center here: https://atlasofsurveillance.org/real-time-crime-centers/detroit-real-time-crime-center

DETROIT PROJECT GREEN LIGHT & THE “NEW JIM CODE”

“A U.S. government study found that even the best facial recognition algorithms misidentify Blacks at five to ten times the rates of whites. In Detroit, at least two individuals, **Michael Oliver and Robert Williams**, have been **wrongly accused** through Project Green Light surveillance technologies of involvement with crimes they had nothing to do with.”

“In June 2019, the Detroit Digital Justice Coalition released a study, “A Critical Summary of Detroit’s Project Green Light and its Greater Context,” that has been widely circulated. As a result, the Detroit Board of Police Commissioners passed a policy in 2019 for the use of facial recognition software. Under the new policy, DPD cannot use facial recognition for live feeds or immigration enforcement, nor can they use the software on mobile devices.”

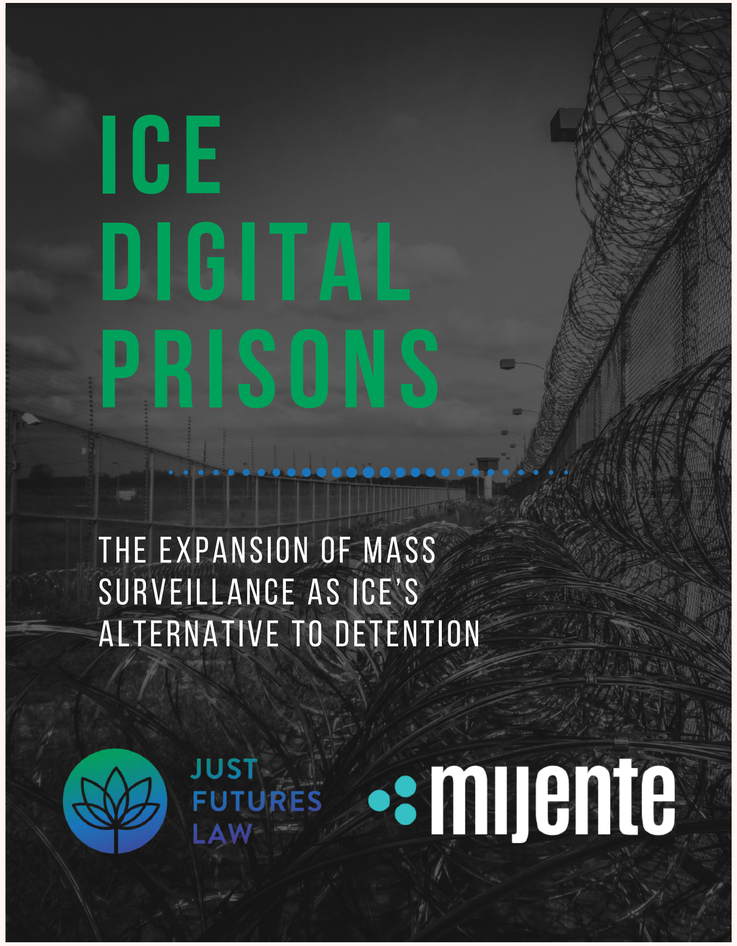
Since the first cameras went live in eight gas stations on January 1, 2016, the system has grown as of April 2020 to nearly 700 locations across the city.

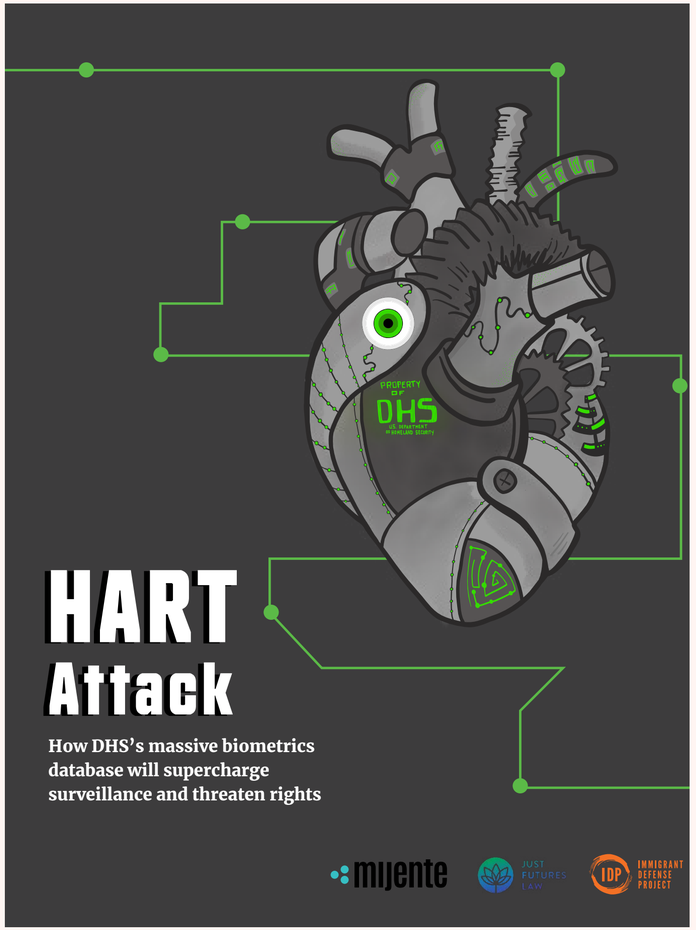


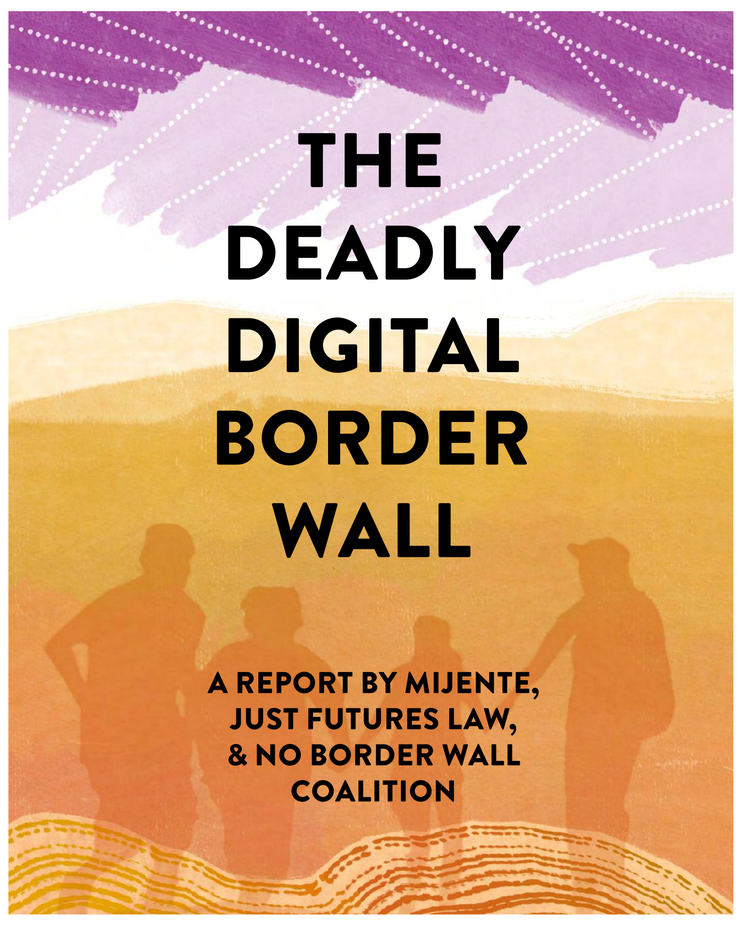
https://publicseminar.org/essays/detroits-project-green-light/

Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time
https://www.vice.com/en/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time

TECH DANGERS FOR PEOPLE ON THE MOVE







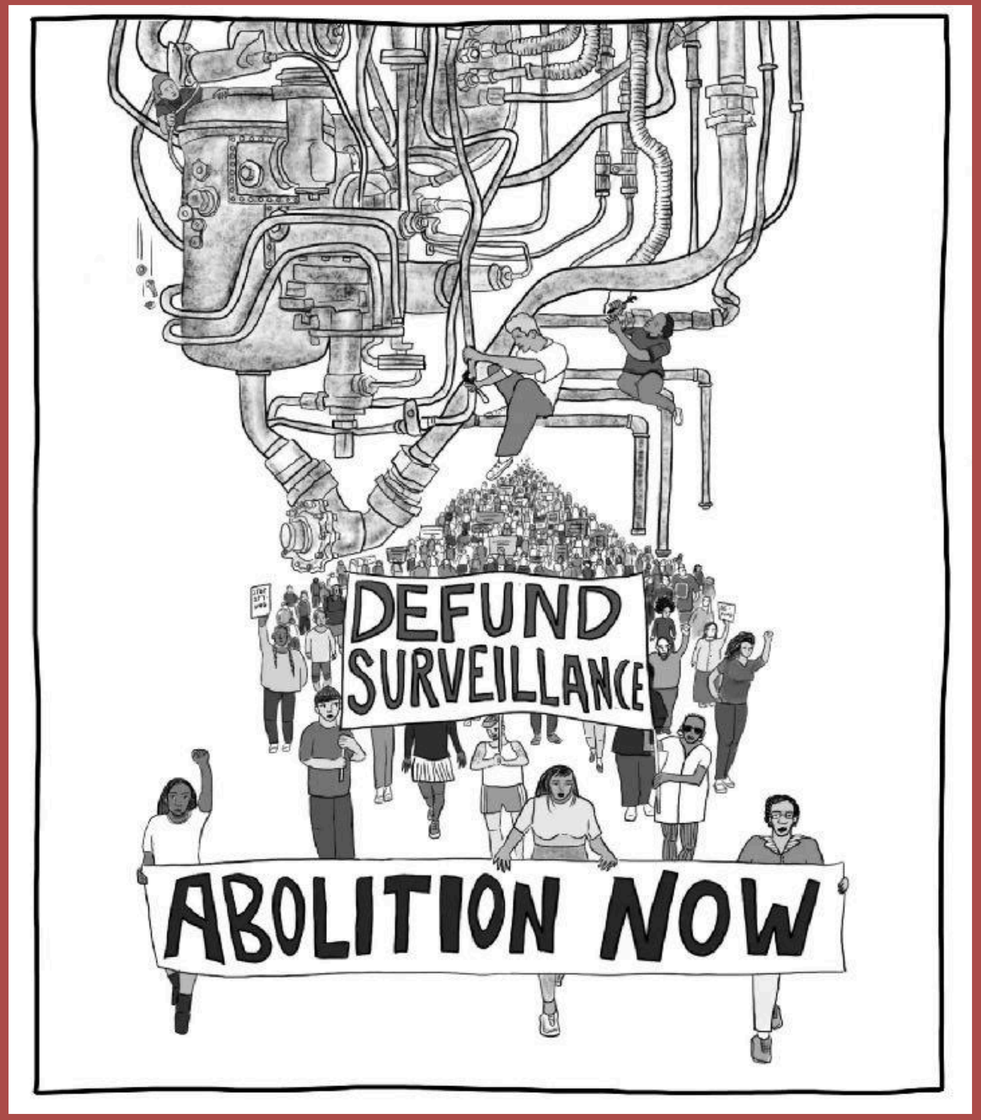
View **The Deadly Digital Wall Webinar** recording:
https://www.youtube.com/watch?v=VDW0lp98-18

No Tech for ICE campaign reports: notechforice.com/resources/

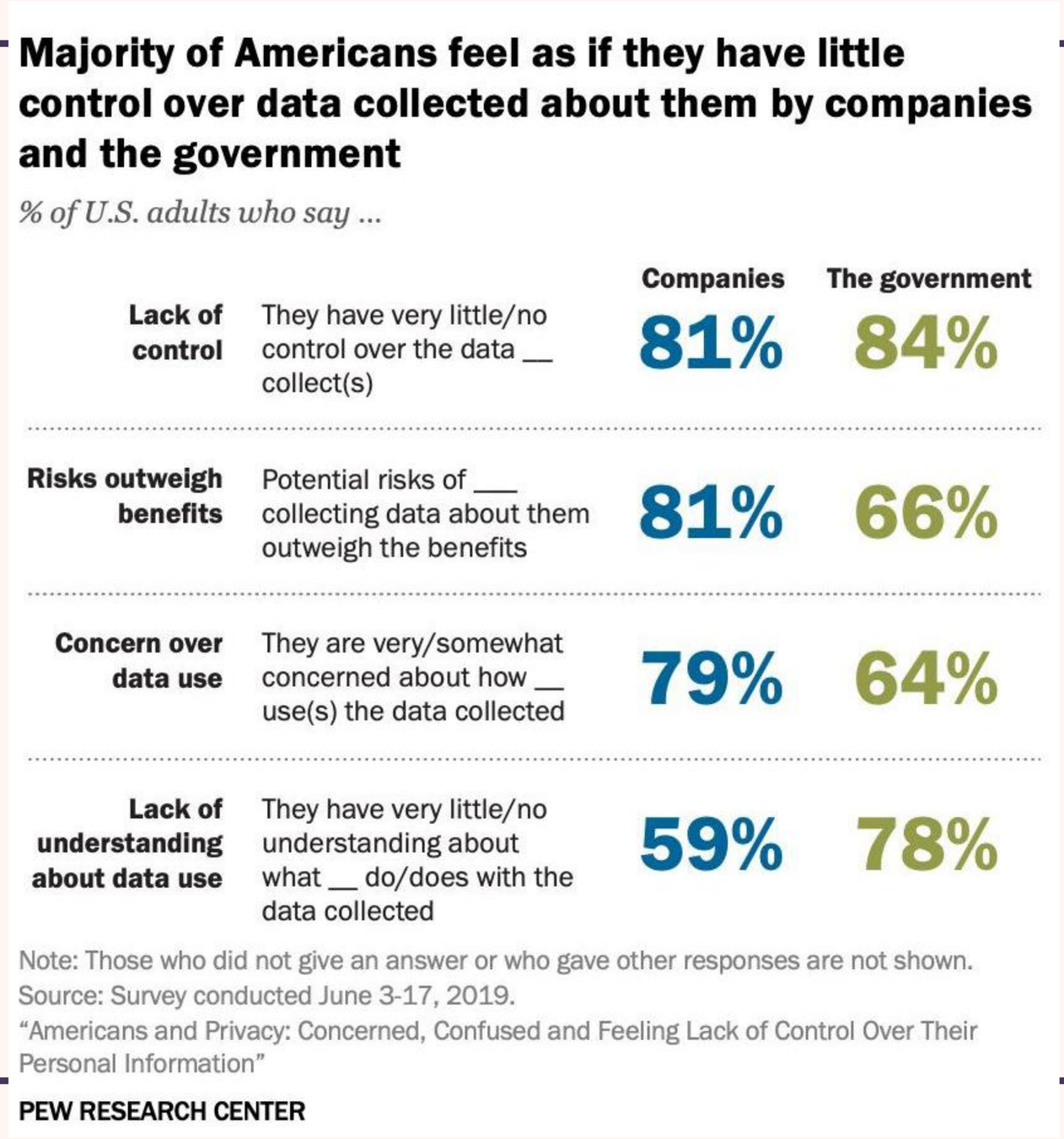
HOW BIG TECH IS HELPING IMMIGRATION AND CUSTOMS ENFORCEMENT (ICE) DO IT’S JOB

https://youtu.be/EEMK4w1A_zo

WHAT IS BEING DONE?

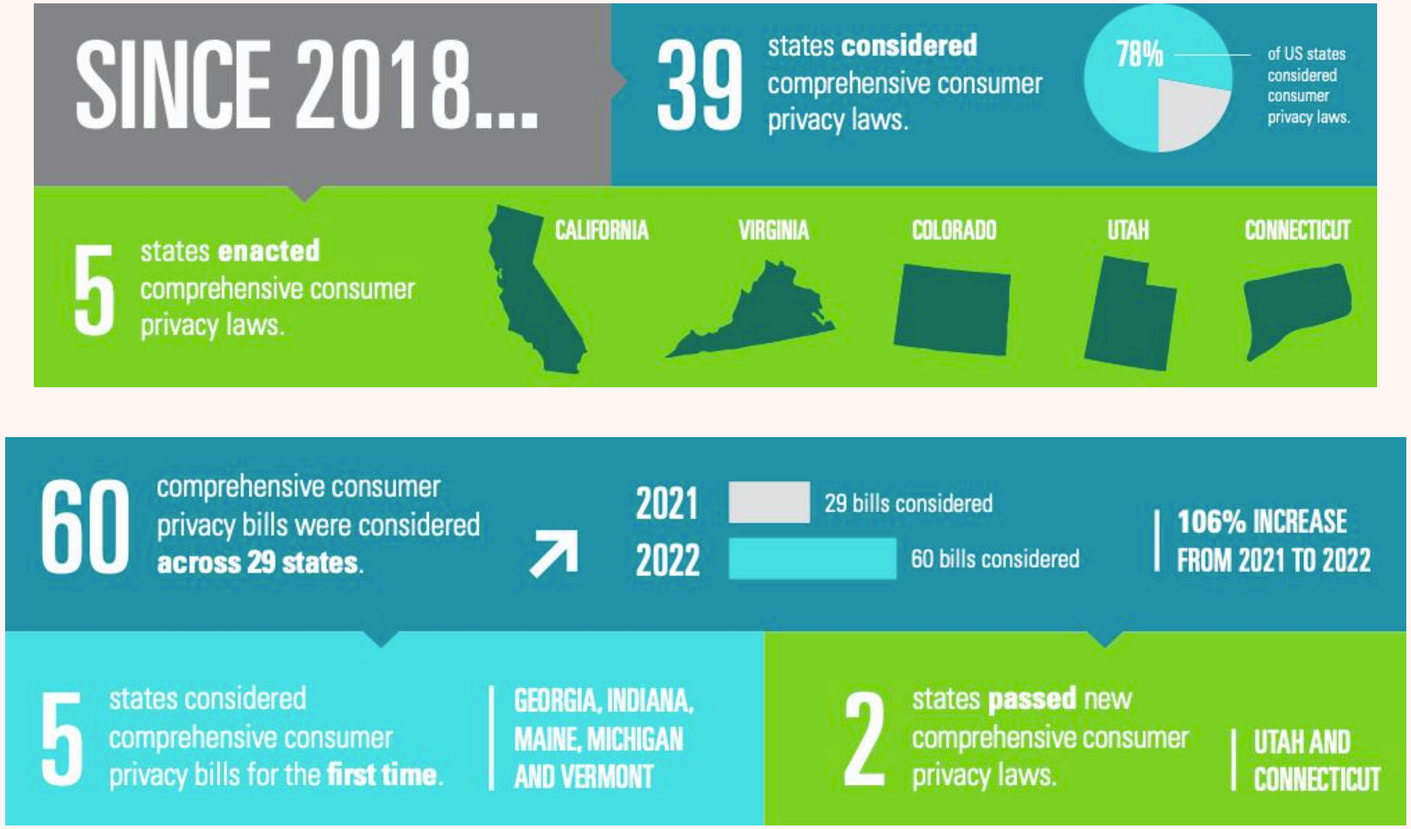


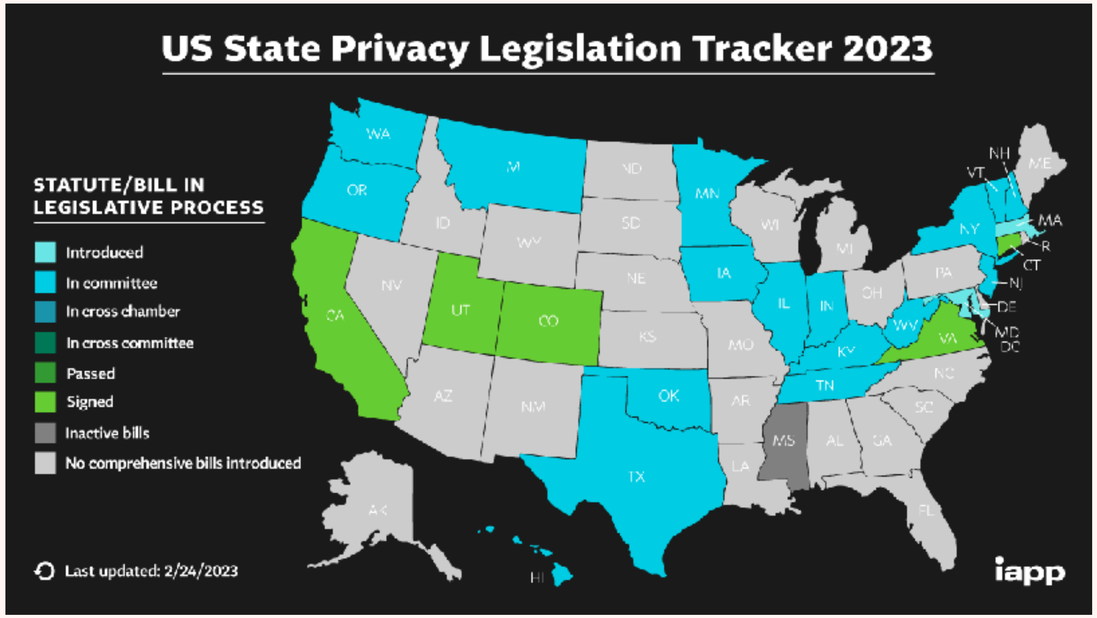
MANY PEOPLE FEEL HELPLESS ABOUT THE DATA OVER-SHARING PROBLEM



PRIVACY LEGISLATION BY STATES

https://iapp.org/resources/article/us-state-privacy-legislation-tracker/





See also **Federal Level Privacy Legislation Tracker**: https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/

ACLU AND THE COMMUNITY CONTROL OVER POLICE SURVEILLANCE (CCOPS) MODEL

https://www.aclu.org/legal-document/community-control-over-police-surveillance-ccops-model-bill

- **The American Civil Liberties Union (ACLU) created a model legislation template for cities to use in their own efforts to push for transparency and oversight.**
- **The Community Control of Police Surveillance (CCOPS) model has been adopted by the city of Oakland and their Privacy Advisory Commission (PAC) in the form of their Surveillance and Community Safety Ordinance, and serves as the basis for New York City's current proposed Public Oversight of Surveillance Technology (POST) Act.**
- **Overall, 12 cities across the US have passed legislation based on the CCOPS model, with over a dozen other cities currently considering adopting this legislation.**

CITY-LEVEL RESPONSES

- **Local organizers have been developing policies to require oversight or banning of surveillance technologies**

- **Mijente and Just Futures Law have produce a guide for organizers (see link below)**

ORGANIZER STEPS

STEP 1

EDUCATE YOURSELF ABOUT THE TECHNOLOGIES CURRENTLY BEING USED AND THEIR IMPACT

- Do background reading and research
- Connect with organizations working on policing and surveillance issues
- Understand which government offices buy surveillance tech
- Understand some basics about how ICE operates in your city.

STEP 2

START THE PROCESS OF COLLECTING THE EVIDENCE FOR YOUR CITY

- Research information that's already been made available by other organizations
- File a public request to obtain government documents
- Analyze the government documents to understand the data, tools, tactics being used as well as the companies and government agencies involved

STEP 3

USE POLICY ADVOCACY AS A TOOL IN THE FIGHT AGAINST BAD TECH

- Educate and move elected officials to understand the issue with the information and analysis you've provided
- Build enough support to request that elected officials launch their own inquiries
- Consider the range of policy options or solutions that already exist to help inform your demands and local organizing
- Get your local government to pass an anti-surveillance resolution and/or ordinance

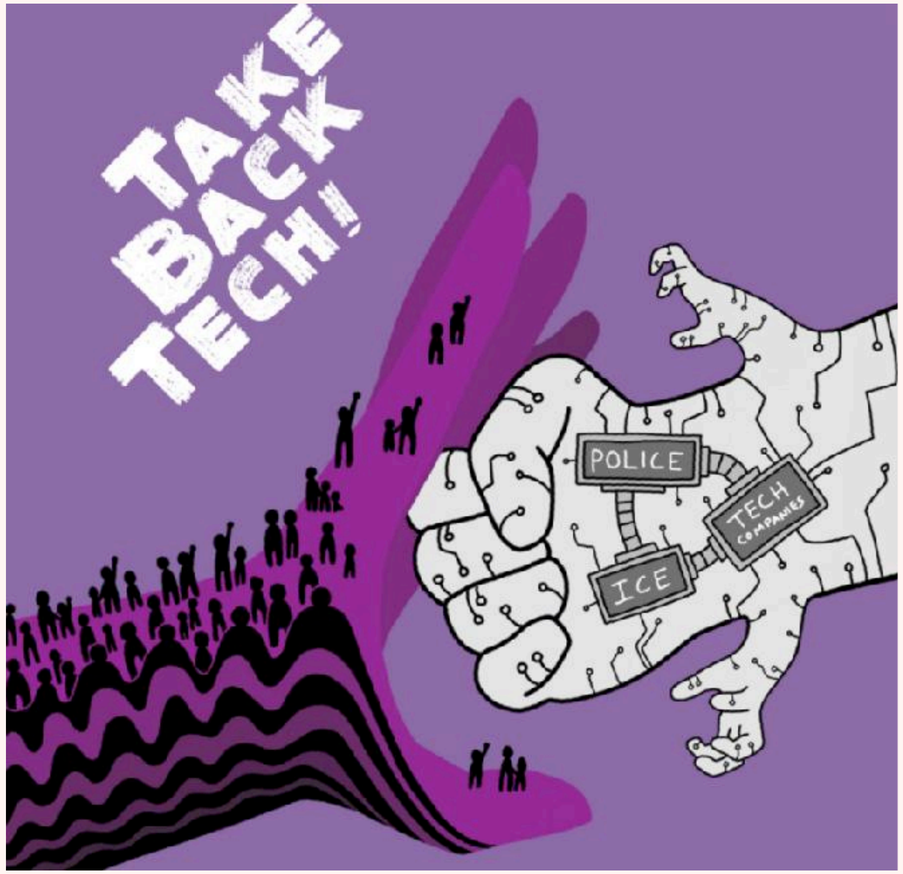
https://mijente.net/wp-content/uploads/2019/07/Tech-Policy-Report_v4LNX.pdf

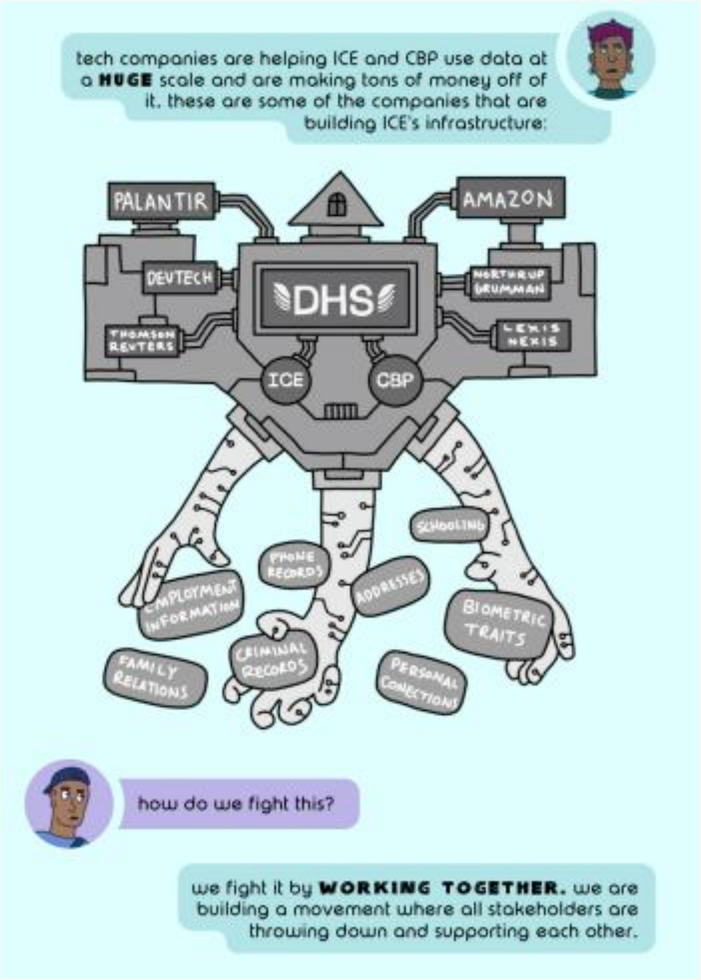
NO TECH FOR ICE CAMPAIGN

https://notechforice.com

Mijente's Not Tech for ICE campaign started in 2018 to disrupt the alliance between tech and immigration enforcement.

COMIC BOOK FOR YOUTH (& ALL)





Get it here: https://drive.google.com/drive/folders/1umhO0e9bpFMcD5FnGjg7zAZHrkebRNye

ORGANIZING BY STUDENTS

OVER 40 campus actions have been taken in recent years

Helping college students identify contracts their university may have with Palantir and demand that their university cancel their contract and that Palantir cancel its contract with ICE

Organizing an international day of action where students in the UK and USA protested Palantir

https://notechforice.com/studentpower/

PRESSURE ON BIDEN ADMINISTRATION TO DO BETTER

JUST FUTURES LAW

JUST FUTURES LAW

el Comité miente

END ABUSIVE SURVEILLANCE OF IMMIGRANT, BLACK & BROWN COMMUNITIES

The Biden Administration must intervene in the massive, militarized technological surveillance machine being deployed against immigrant, Black and Brown communities. The parade of horribles--from Clearview AI to Palantir to Border Patrol drones surveilling Black Lives Matter protesters over Minneapolis--make clear that DHS is working in collaboration with tech companies to build a massive surveillance apparatus to track and criminalize both immigrants and U.S. citizens alike.

STOP USING INVASIVE TECH COMPANIES

End all contracts, agreements, and pilot initiatives with tech companies that build the technology and surveillance programs that lead to DHS enforcement - such as Palantir, Clearview AI, Vigilant Solutions, and Thomson Reuters.

BAN INVASIVE DATA COLLECTION & SURVEILLANCE

Strike memoranda, rescind regulations and cancel contracts and/or agreements that authorize invasive technologies such as DNA collection, facial recognition, social media surveillance, and other biometrics collection.

RESTRICT UTILITY & ESSENTIAL SERVICES DATA

Issue memoranda limiting ICE from accessing or using the data of essential or life-saving services (e.g. gas, water, internet, and other utilities services, health services, or motor vehicle licensing) for immigration enforcement.

REDUCE BY 50% DHS SURVEILLANCE SPENDING

Halve the amount of funding requested from Congress for DHS biometrics and surveillance programs and equipment in FY 2021.

CONDUCT A PRIVACY AUDIT OF DHS

Conduct a privacy audit on DHS and its contractors that collect, analyze, share, store, or purchase personally identifiable information for ICE, CBP, and/or USCIS and provide audit results to the public. This should include requiring DHS to provide a list of all contracts, contractors, use, and monies deployed for surveillance and technologies.

Regulating corporations who violate the human rights of immigrants and communities of color should be an important marker of reform for this Administration.

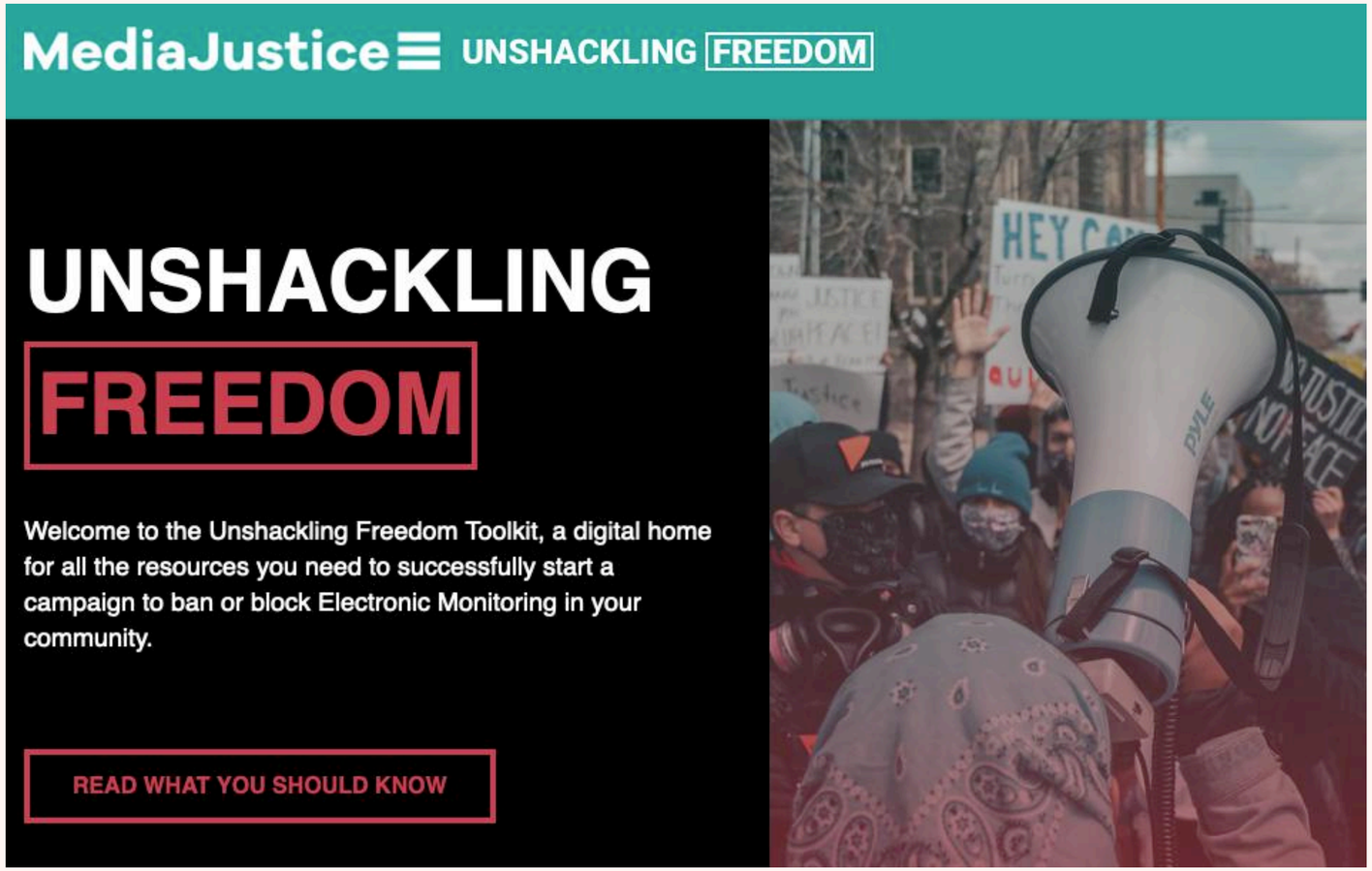
https://www.justfutureslaw.org/s/FORMATTED-Biden-Demands-Tech-Surveillance-Rec.pdf

CAMPAIGN AGAINST ELECTRONIC MONITORING TECH

https://mediajustice.org/unshackling-freedom/what-you-can-do/

How To Build An Unshackling Freedom Campaign: A Roadmap

- ☑ Understand the Local Landscape
- ☑ Set Goals
- ☑ Identify key players
- ☑ Develop Messaging
- ☑ Make a Call To Action
- ☑ Talk to the Media
- ☑ Take it Online
- ☑ Organize IRL



CALL TO CANCEL ICE CONTRACTS WITH LEXISNEXIS

- **February 2023 call to action**
- **80 immigrant rights, racial justice, government accountability, human rights, and privacy organizations have signed it**
- **Quaker group AFSC (American Friends Service Committee) is one of the signatories**

epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

EPIC, Coalition Call for ICE to Cancel Contract with LexisNexis for Invasive Surveillance Databases

February 23, 2023

In a letter signed by more than 80 immigrant rights, racial justice, government accountability, human rights, and privacy organizations, EPIC and coalition members called upon ICE not to renew a $22 million contract for a suite of surveillance services. LexisNexis gives ICE agents access to the Accurint database compiled from thousands of sources and includes billions of government records, utility bills, phone records, medical records and more. ICE uses Accurint as well as other LexisNexis tools to surveil immigrants and

https://edri.org/our-work/protectnotsurveil-eu-must-ban-ai-uses-against-people-on-the-move/

EUROPEAN DIGITAL RIGHTS WORK

Pressure is growing on the EU parliament to prohibit the use of AI to profile and "push back" migrants

#ProtectNotSurveil: EU must ban AI uses against people on the move

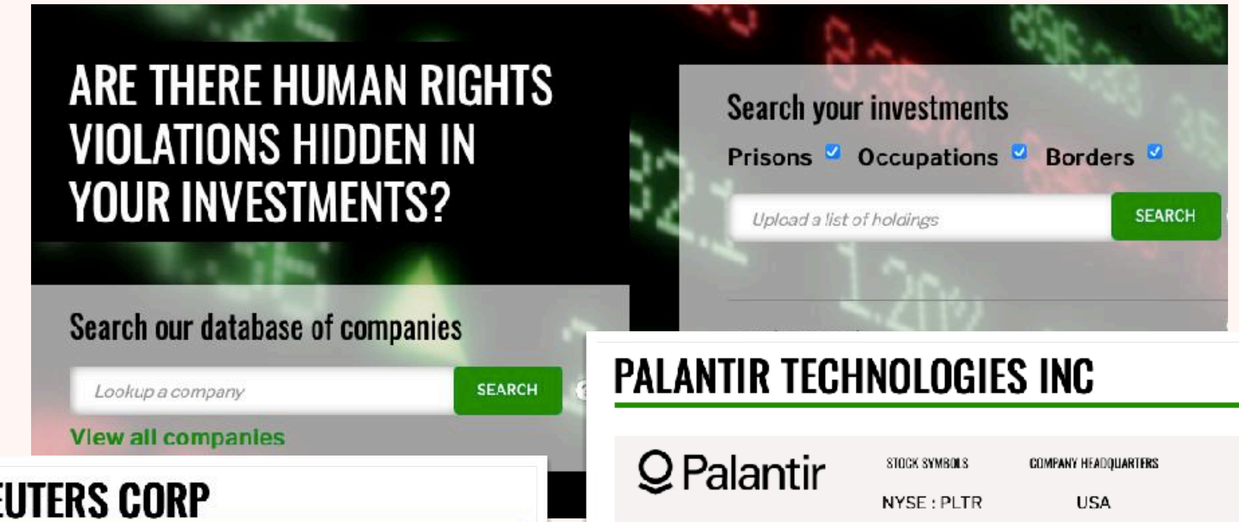
From AI lie-detectors, AI risk profiling systems used to assess 'risky' movement, and AI for illegal pushbacks, to the rapidly expanding tech-surveillance complex at Europe's borders, AI systems are increasingly a feature of migration management in the EU.

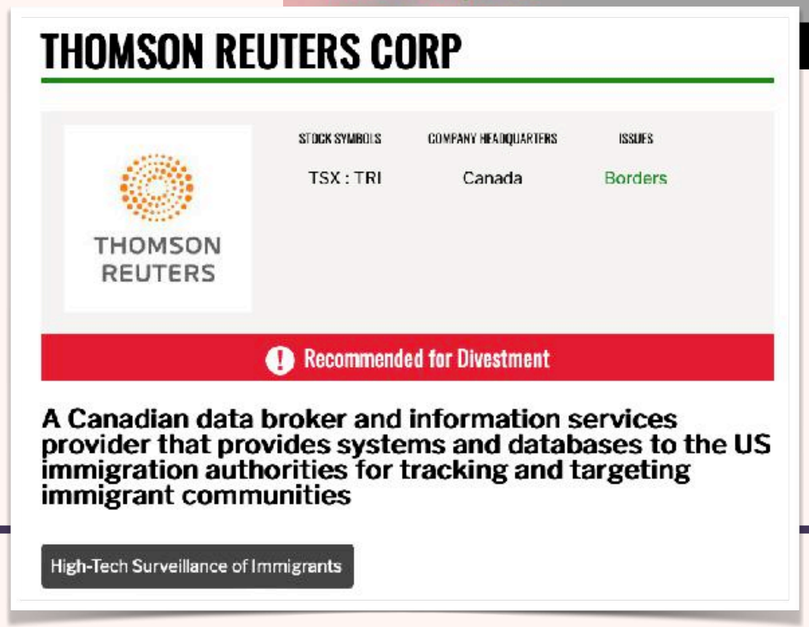
195 organisations and individuals, led by EDRi, Access Now, Refugee Law Lab and PICUM, support our open letter calling on the EU to make significant changes to the EU AI Act, better addressing the harms of AI when used in the context of migration.

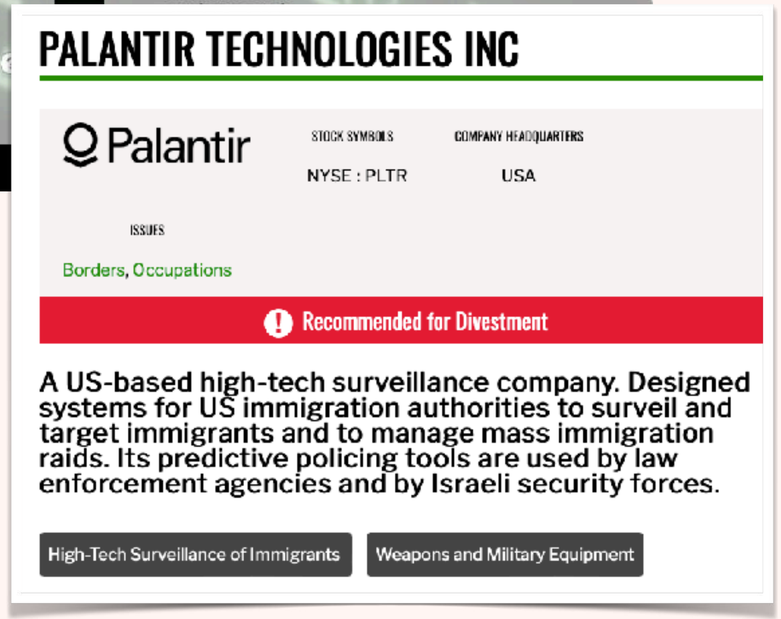
AFSC INVESTIGATE TOOL

https://investigate.afsc.org/

- **The American Friends Service Committee has built a tool to help investors research companies doing work that goes against their values.**
- **The tool can help individuals and groups decide whether they want to divest from a company or put pressure on the company to change it's policies**





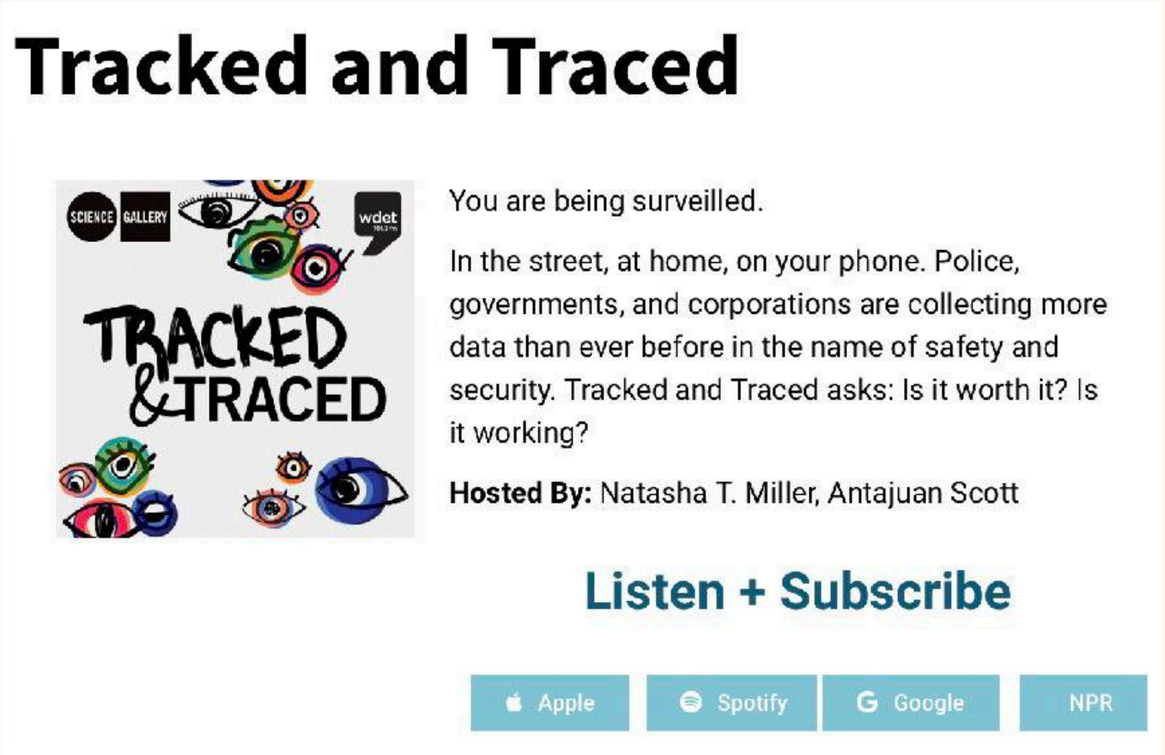


RESOURCES

TRACKED AND TRACED PODCAST

EPISODES LIST (series ended in Aug 2022)

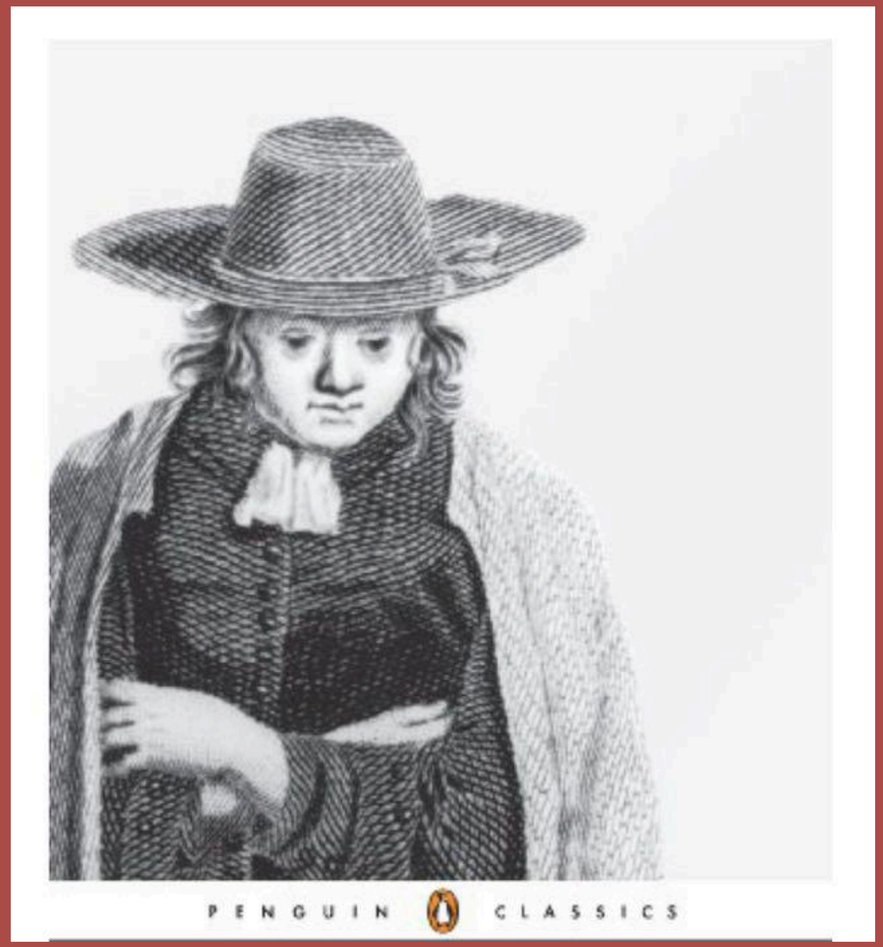
- Reporting on surveillance in Detroit
- Are hundreds of parking meters quietly surveilling Hamtramck residents?
- How a ban on Chinese drones could set back wildfire fighting in the U.S.
- The case for digitizing the foster and adoptive systems in the U.S.
- Sousveillance and the price of virality
- Safety vs. Surveillance in Dearborn Public Schools
- You are the product, thanks to surveillance capitalism
- Does ShotSpotter prevent violent crime in Detroit?
- Does Project Green Light in Detroit reduce crime?
- How thousands of American Muslims ended up on the terrorist watch list



https://wdet.org/podcasts/tracked-and-traced/

- Tactical Tech's *What the Future Wants* interactive youth-focused exhibit: theglassroom.org/what-the-future-wants/ (includes kit to host your own event)
- The EFF Atlas of Surveillance: atlasofsurveillance.org/
- EPIC (Electronic Privacy Information Center) Surveillance Oversite project: epic.org/issues/surveillance-oversight/
- Tracked and Traced Podcast: wdet.org/podcasts/tracked-and-traced/
- No Tech for ICE reports: notechforice.com/resources/
  - Free Tech Wars Online Course offered by #NoTechforICE: instituto.mijente.net/courses/tech-wars/
- Just Futures Law: justfutureslaw.org/our-work
- Blacklight Tracker Website Inspector: themarkup.org/blacklight
- Our Data Bodies project (includes Detroit focus): odbproject.org
- The Markup Privacy Series: themarkup.org/series/privacy

GREAT RESOURCES



THANK YOU

Bill Warters
leymworker@gmail.com

Slides and recording will be posted to LEYM Interest Group page:
https://leym.org/pje-interest-group/