UNFRIEND THE NYPD

It's never been easier for police to spy on millions of people at once. This guide explains how police can spy on you through your phone, and how you can protect yourself and your community.

PUBLIC ACCESS DESIGN

Why should I care if police see what's on my phone? I don't break the law.

They shouldn't be looking at our phones in the first place. Police need a good reason to search our stuff. They're surveilling us!

(When police spy, it's called "surveillance.")

Idc, let them look. If I'm not doing anything wrong I can't get in trouble.

That's not necessarily true. Policing in the U.S. is discriminatory. That means you could be targeted because of what you look like, who your friends are, or where you work, live, or pray.

Even if you're not doing anything wrong, you could be targeted and harassed, arrested, or deported.

fr?

Maybe you don't care if they're watching you personally. But if your phone is unprotected, **you could help police surveil other people**, putting your friends and family at higher risk.

AT RISK FOR BEING ME

Your risk profile is how likely you are to be spied on by police. Every one of these you check off puts you at risk.

Police are more likely to spy on you if you...

Identify as...

- Black
- Latina/o/x
- Muslim
- LGBTQIA+
- an immigrant/refugee

Live in a neighborhood thats...

- Black, Indigenous, immigrant, and/or people of color
- low-income
- touristy

Have recently been to...

- an airport
- a protest
- a mosque
- a concert or large event

Have ever posted about...

- Defund the Police
- Black Lives Matter
- ANTIFA
- left leaning/progressive politics

PROTECT YOURSELF AND YOUR COMMUNITY

Knowing your risk profile can help you decide which actions to take to protect yourself and your community. Use this guide to learn how police can surveil your phone through social media, messaging apps, and geofences.

HAS ANYONE EVER TREATED YOU UNFAIRLY BECAUSE OF THE WAY YOU LOOK?

Police target people based on things they see on your social media accounts. They make assumptions about who you are, your political views and beliefs, and who you spend your time with. Police can do this online without a warrant.

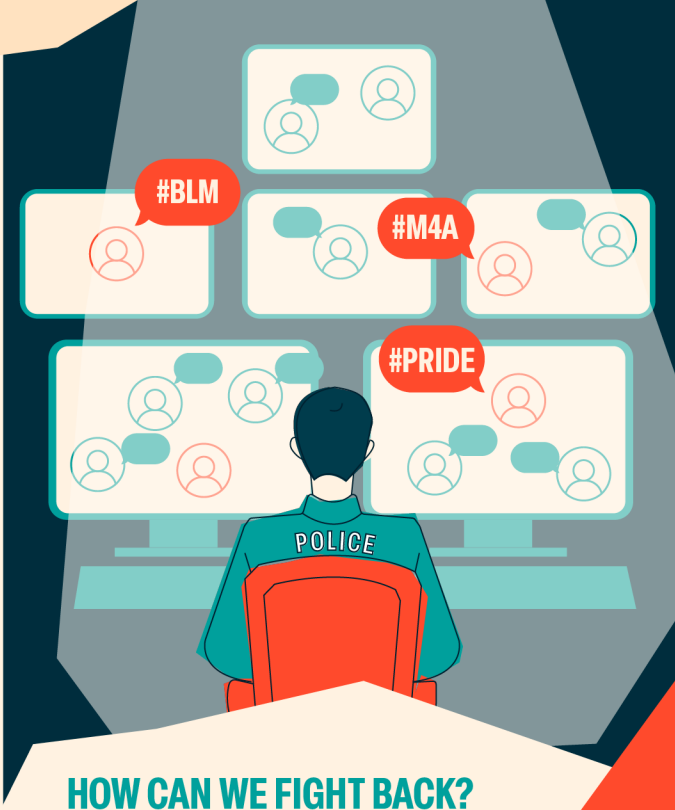
HOW SURVEILLANCE HAPPENS

Public information: Any public account is available for anyone, including the police, to see.

Fake profiles: Police use software to generate thousands of fake social media accounts, and then can follow you or send you a friend request.

Monitoring software: Police use software to make detailed searches, like looking up everyone who used a certain hashtag.

Warrant requests: If your account is set to private, police can ask app companies (like Facebook and Twitter) for info from your social media account.



HOW CAN WE FIGHT BACK?

- Don't accept friend requests from strangers, and set your social media profiles to private—that includes Venmo, CashApp, and PayPal too.
- Ask permission to tag people in your posts. Don't tag people in photos during protests.

HAS ANYONE EVER GONE THROUGH YOUR PHONE WITHOUT YOUR PERMISSION?

Police can read the messages you send and receive and use them against you.

HOW SURVEILLANCE HAPPENS

Police can gain access to your messages: They need permission from one of the people in the conversation or a warrant.

Messaging platforms see your messages: If the messages aren't end-to-end encrypted, they can turn them over to the police.

***End-to-end encryption** means that no one else can see your messages, not even the platform you're messaging on. Even if the police were to get a warrant, the platform wouldn't be able to turn over your messages.*

Not all encrypted messages are end-to-end encrypted. Some types of encryption protect your messages' content, but not your location or other details. Some companies say they're end-to-end encrypted, but they can break that encryption and give your info to the police (WhatsApp).

HOW CAN WE FIGHT BACK?

- Only use platforms that are truly end-to-end encrypted, like Signal.
- Save sensitive conversations for in-person conversations.

HAVE YOU EVER BEEN AT THE WRONG PLACE AT THE WRONG TIME?

Geofences are when police draw a line around an area on a map and make a list of all the phones that passed through during a certain period of time. When police use geofences, lots of innocent people become potential suspects, including vulnerable communities like undocumented people and and people who have been arrested or incarcerated.

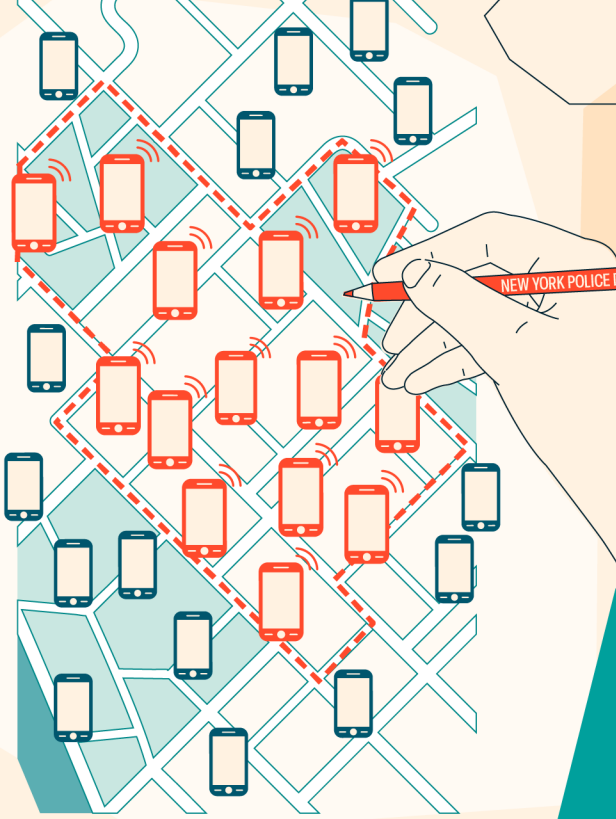
HOW SURVEILLANCE HAPPENS

Apps can monitor your location: For example, the default setting on your Google account automatically keeps track of your location history.

Police get a geofence warrant: The warrant demands that app companies hand over to police a list of all the active accounts that passed through a specific area.

Police buy data: If a judge won't sign off on a warrant, police can buy the data from data brokers (companies that collect and sell data).

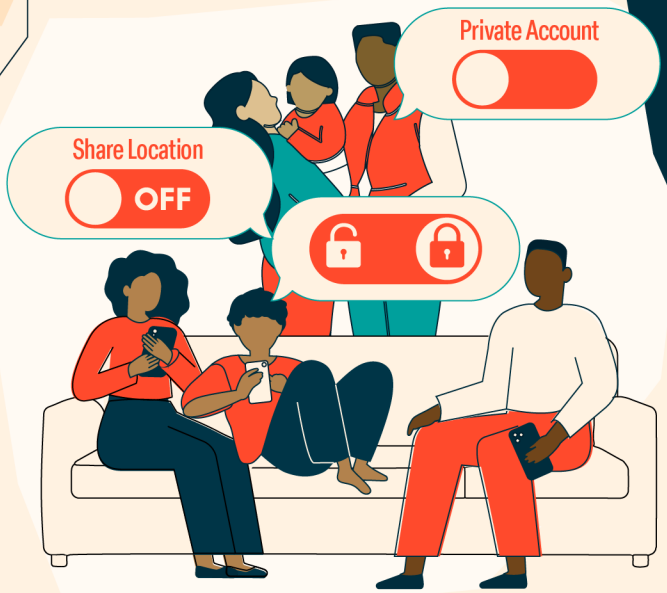
The number of geofence warrants is growing. *Google received nearly 12,000 geofence warrants in 2020, and they are now the number one type of warrant Google receives in the U.S.*



HOW CAN WE FIGHT BACK?

- Limit the apps that can access your location data as much as possible.
- Keep your phone on airplane mode at protests and other sensitive locations.

PROTECT YOURSELF, YOUR FRIENDS, AND YOUR FAMILY



Even if your phone is protected, you won't be 100% secure as long as policing is discriminatory and they can track what you do. ***The only way to end police surveillance is to change government policy.***

OK so what can we do?

To *rly* fight back, we have to push back as a community against police surveillance.

Advocate for bans on social media monitoring and geofence warrants.

Pressure companies to make their platforms end-to-end encrypted.

Right. But what's the first step?

Check in with groups that are already active, like S.T.O.P. Learn more about their campaigns and how to volunteer: **stopspying.org/our-campaigns**

It's really important to teach your family members how to make their phones safer by following the tips in this booklet.

ok gotchu fam

This project was produced through **Public Access Design**, a program of the **Center for Urban Pedagogy (CUP)**. Public Access Design projects use design to make complex urban issues accessible to the New Yorkers most affected by them.

The Center for Urban Pedagogy (CUP) is a nonprofit that uses the power of design and art to increase meaningful civic engagement. ***welcometocup.org***

The Surveillance Technology Oversight Project (S.T.O.P.) fights to abolish local governments' systems of mass surveillance, highlighting the discriminatory impact of surveillance on New York's communities. ***stopspying.org***

Aishwarya Srivastava is a NYC based designer.

CUP: Agustín Cepeda, Onyi Egbochue

S.T.O.P.: Albert Fox Cahn, Sam Van Doran, Evan Enzer, Leticia Murillo

Designer: Aishwarya Srivastava

Big Thanks: Patrice Allen, Wael Dkhili, Aaron Dover, Christian Ibanez, Justina Ibanez, Lynette A. Lewis, Abdiel Paulino, Daniel Sardinha, Khamel Terry, Dylana Bourne, Faith A., Renayah Fernandez, Anaiyah, Mystic, Riyah, Ann, Raysha Vasell Frazier, and Ariel Ulloa (community members)

Support for this project was provided by public funds from the New York City Department of Cultural Affairs in partnership with the City Council and Council Members Brad Lander and Antonio Reynoso.

© the Center for Urban Pedagogy, 2022