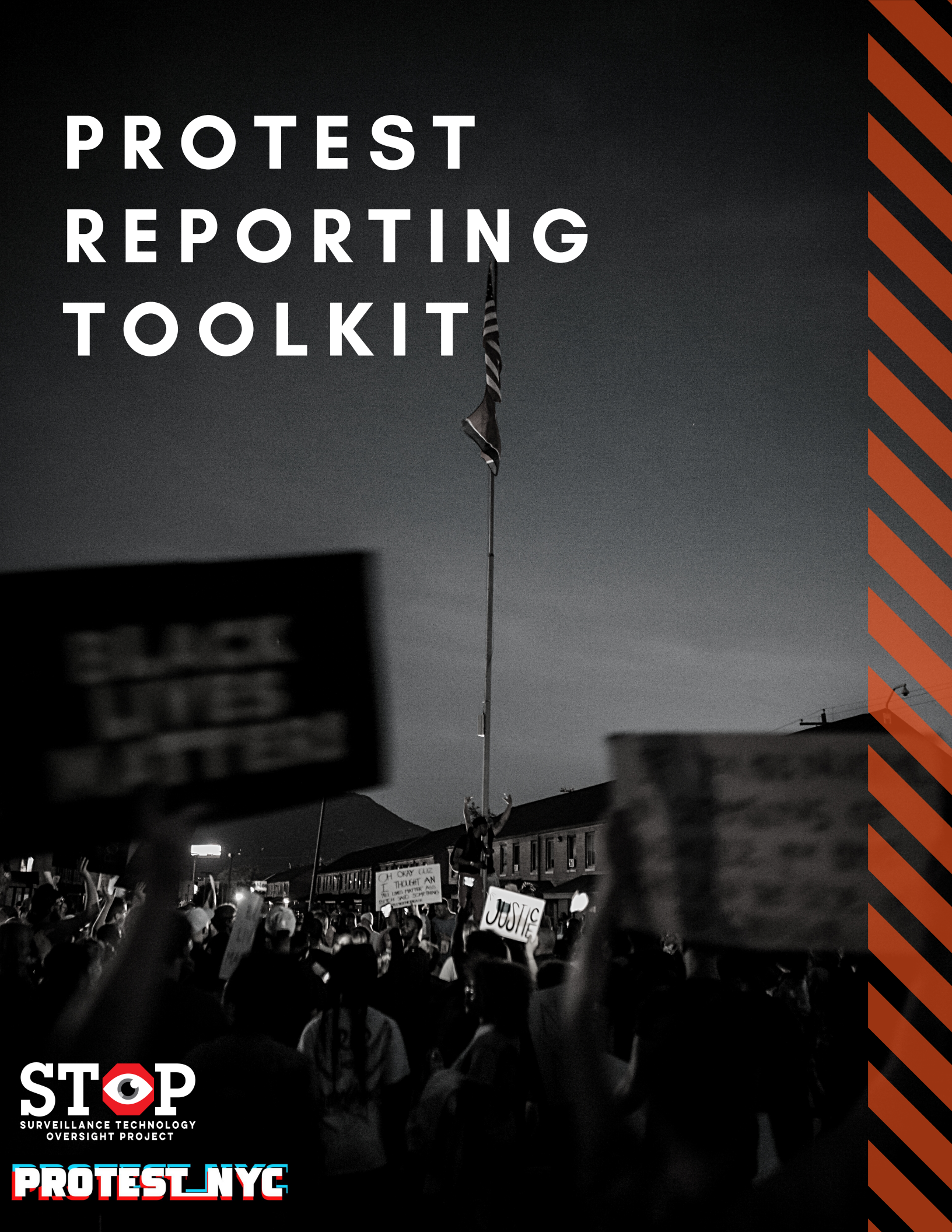
PROTEST REPORTING TOOLKIT



STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

PROTEST_NYC

PROTEST REPORTING TOOLKIT

When you attend protests, law enforcement use surveillance technology to monitor your social media, break into your phones, and track your location. Law enforcement routinely target peaceful protesters with these destructive measures. But you can take these steps to keep yourself and your sources safe.

USE YOUR RIGHT TO REPORT RESPONSIBLY

Protests are often led by and composed of over-policed and historically-marginalized people, including Black, Indigenous, undocumented, brown, and LGBTQ+ activists, and those experiencing mental and physical disabilities.

Innocent protesters are frequently arrested despite not committing any crime, and identifying photos and videos from a demonstration could cause serious harm to them and their families.

In addition to facing arrest, protesters may be targeted for deportation, have their immigration or employment statuses compromised, be targeted by hate groups, or be fleeing intimate-partner violence/domestic abuse.

Finally, private tech companies collect images and personal data on their platforms while developing AI that tracks, identifies, and monitors users online. Some companies even have data-sharing relationships with law enforcement.

STOP SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT
PROTEST_NYC

PROTEST REPORTING TOOLKIT

PRACTICE SAFE PRESS ETIQUETTE

- Don't crowd people with cameras
  - Crowding or rushing people can lead to chaotic and stressful situations or increased police attention. It can also erode the community's trust in you as a responsible reporter
  - Consider recording from a distance and/or asking individuals if they're comfortable being on camera
  - Don’t antagonize protesters who establish boundaries with you. Give them space when they say they need it

- Redact information that may identify individuals
  - If you did not confirm with an identifiable individual that they are comfortable being on camera or being published in any way, redact information that could be used by malicious parties. This includes faces, tattoos, unique hair and accessories/clothing, and brand names
  - Mistakes happen. If someone asks you to remove or redact something, work with them to resolve the issue

- Live stream responsibly
  - If you are streaming live, the people around you should be aware
  - Live-streaming can endanger the safety and security of an entire area if malicious actors are viewing
  - Live-stream broadcasts cannot be redacted. Audiences can also rip streams and clips. Mistakes in reporting and documentation made on live-stream could be permanent

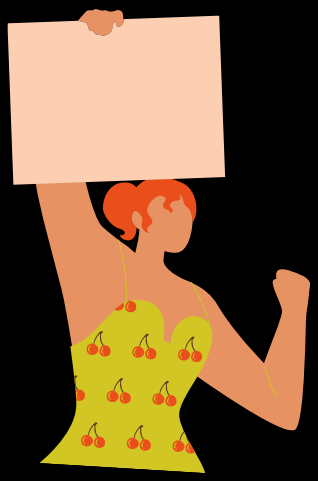
- Record crowds from behind and/or below the shoulder to minimize identifiable information
  - This expedites the redaction (e.g. blurring) process
  - Photos are faster and easier to redact than videos
  - Record audio or take notes on paper or a secure device for accurate reporting

STOP SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT
PROTEST_NYC

PROTEST REPORTING TOOLKIT

PRACTICE SAFE PRESS ETIQUETTE (continued)

- Communicate clearly with the people around you
  - This includes organizers, police, medics, legal observers, and fellow members of the press. Do not endanger yourself or others while trying to get your shot
  - If organizers ask you to stay in a given position, don't antagonize them. If you need to move around, explain why politely and clearly
  - Model the respectful behavior you'd like to see, and receive, while you work

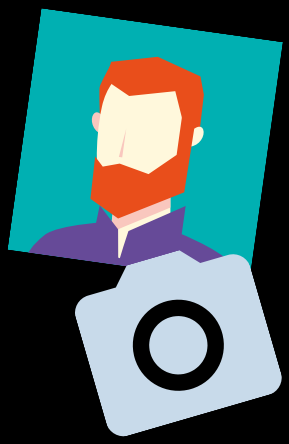


- Don't deceive protesters while covering them
  - When asked your name, give the one most commonly associated with your work
  - Be clear about which publication you're from while on assignment. If you freelance, be reasonably specific about your clients
  - If a protester doesn't appreciate your work or employer, ask what you can do to help. Again, do not endanger yourself or others while working

IDENTIFYING FEATURES + INFORMATION

Problems:

- Identifying Features - As technology evolves, so too does the ability to quickly and accurately identify persons in a photograph. While facial recognition is becoming an increasingly accurate method for automating this process, other technologies provide methods to automate the identification of individuals based on other identifying features such as tattoos and biometrics



- Seemingly Benign Information - Information that otherwise seems benign can be used to identify the individual to whom it pertains, especially when cross-referenced with other available data

STOP SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT
PROTEST_NYC

IDENTIFYING FEATURES + INFORMATION (continued)

Sample Tools

iOS

- Native photo editing functionality can be used to paint over faces and other identifying information
- There is no native functionality to remove metadata and geotagging, but users can take a screenshot of the edited photo or screen record an edited video and then delete it to ensure there is no metadata attached

WhatsApp

- Removes metadata from photos and videos before sending

YouTube

- Free-to-use blurring tool for videos. Videos can be downloaded and then shared on other media. However, metadata will need to be removed before uploading the video. SMS metadata identifies the parties to the communication

Signal

- Native feature to blur faces in photos taken through the app
- Removes metadata from photos and videos before sending

IDENTIFYING FEATURES + INFORMATION (continued)

Sample Tools

Windows

- Can be used to remove metadata from photos or videos

Android

- Native photo editing functionality can be used to paint over faces and other identifying information
- There is no native functionality to remove metadata and geotagging, but users can take a screenshot of the edited photo and then delete it to ensure there is no metadata attached
- Some Android phones have native screen recording functionality

Telegram

- Removes metadata from photos and videos before sending

Image Scrubber

- Users can selectively blur parts of photos and remove the metadata
- Open source and hosted by GitHub
- All image processing happens in the browser
- Can be used without a data connection (e.g., with airplane mode enabled)
- Works on Windows, MacOS, iOS, and Android

PROTEST REPORTING TOOLKIT

ANTI-DOXING BEST PRACTICES

- Delete apps that may track your location (Ex: Facebook, Twitter, WhatsApp, Google apps, Waze, etc.) If you are going to use these apps on your mobile device, use them in the device's web browser
- Use apps and services that require as little information as possible
- Limit the permissions of installed apps to only what is necessary
- Configure web browsers to delete cookies and browsing history when closed, or use private browsing functionality like 'Incognito Mode'
- Use a VPN that does not maintain logs

CELL PHONE LOCATION TRACKING

Problem:
The mere presence of a cell phone could lead to the identification of sources and protesters through reverse engineering of location data

Airplane Mode:
Airplane mode turns off the phone's location services and disables Wi-Fi, GPS, NFC, Bluetooth, etc. which could otherwise be used to track the holder's location even if the phone is turned off

PROS	CONS
Helps prevent a third party from reverse engineering a source's identity, who was present at a covered event, etc. from location data Your cell phone can still be used to record information such as notes and interviews	You cannot report on events as they unfold because your phone is unable to communicate, leading to underreported or delayed reporting about abuses by relevant actors like the police

STOP SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT
PROTEST_NYC

MESSAGING

Problems

- SMS messages are insecure because they are unencrypted and can easily be intercepted
- SMS metadata identifies the parties to the communication

Use secure messaging apps -- *see table below*

	End-to-End (E2E) Encrypted Messages	E2E Encrypted Voice & Video	Open Source?	Self-Destructing Messages?	Metadata required to register?	Other
Signal	YES	YES	YES	YES	Phone #	
Telegram	1-on-1 secure chats only (not default)	YES	Clients and APIs only No back-end infrastructure or encryption protocol	Secure chats only	Phone #	
WhatsApp	YES	YES	Messaging protocol only	YES	Phone #	Owned by and shares data with Facebook, with no opt-out Major 2019 data breach Does not encrypt metadata between endpoints
Wire	YES	YES	Messaging protocol only	YES	Email	Keeps record of everyone a user has contacted until their account is deleted
Confide	YES	NO	No, but independently audited	Automatically after being read		Numerous security problems discovered in 2017
Wickr	YES	YES	YES	YES	Email for Wickr Pro only	

PROTEST REPORTING TOOLKIT

E-MAIL

Problem:
Although email services encrypt messages while they are in transit, most are not end-to-end encrypted. This allows an email service provider to see the content of messages stored on its servers, and to produce the messages pursuant to legal process (e.g., warrant)

Secure Email Providers: ProtonMail, Tutanota, Hushmail, CounterMail

PROS	CONS
Messages are encrypted in transit and at rest so they cannot be read without the encryption keys, even by the vendor and even if they are intercepted by a third party	Some apps allow only a limited number of messages per day, but users can pay a monthly or yearly subscription for more
Some secure email providers are open source, which allows security experts to verify their security	Some apps require users to pay a subscription to use at all (e.g., Hushmail, CounterMail), and others offer advanced features only to paying users (e.g., ProtonMail, Tutanota)
Most providers do not log user activity	
Some providers delete identifying metadata like IP addresses from emails	
Some providers allow users to send password-protected encrypted emails	
Some providers' mobile apps allow users to set timers for automatic message deletion	

QUESTIONS OR TIPS?

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT, INC.

40 RECTOR STREET
9TH FLOOR
NEW YORK, NY 10006
WWW.STOPSPYING.ORG

PROTEST_NYC

PROTEST.NYC
PROTEST_NYC

LINKTR.EE/PROTEST_NYC

NYCPROTESTUPDATES@GMAIL.COM