GOVERNMENT INTRUSION: COMMS TIPS

Meeting safety

- Here's a new Zoom safety backgrounder. Consider adding a privacy disclaimer to every meeting.

- Here are two useful safety backgrounders from Shake Technologies, who specialize in providing cybersecurity and technology consulting for nonprofit and social justice organizations. A) Signal safety backgrounder and B) safety recommendations for international travel.

- Be aware about what AI you have enabled — on your phone, in your office/home environments, etc. Using less "smart" tech could increase your privacy.

- If you or someone in your workplace is using dating apps, share this safety backgrounder.

Reacting to government intrusion

- If you don't already have a plan in place:

    - Prep some messaging that you can swiftly amend if you or your area of focus is targeted.
    - Make a list of all of your internal and external audiences, then map out what communications are needed and who can spearhead what.
    - Prepare to create/edit some background material to help journalists, allies and others add content and nuance to their understanding.

Eliminating and auditing web and social copy

- Auditing the copy on sites you control — web and social — is a good idea. You should also be prepared to edit copy based on the way you may be targeted by government intrusion, so that all of your audiences can clearly understand what you do, how that aligns with the law, and why you do it (your values). Avoid jargon, especially if it can be interpreted in multiple ways.

- It's always a good practice to remove unnecessary content. Your online presence does not need to be a historical archive, it should serve specific audience purposes. If you are removing content for safety or potential intrusion reasons, be clear about exactly why the changes are being made.