PROTECT YOURSELF ONLINE &

TAKE BACK CTRL

A ZINE FOR RECLAIMING OUR RIGHTS IN THE FACE OF GOVERNMENT & CORPORATE SURVEILLANCE

PRESENTED BY THE ELECTRONIC FRONTIER FOUNDATION

INTRODUCTION

Good digital practices begin with knowledge about your own situation and that of your community—whether you're communicating in your family group chat or planning a protest with friends.

Figuring out where to start might feel overwhelming, but a few simple steps can go a long way to better protecting your privacy and building an online space that feels as free and safe as speaking with people close to you in real life. Together, we can make changes to protect ourselves and our communities. And to help, we've put together tips for four common situations where you can reclaim your rights.

TAKE BACK CTRL

WHEN SENDING MESSAGES

Sooner or later we all need to send a message that absolutely must be safe from prying eyes, but why wait for that moment to arrive? Start using a secure, encrypted platform now for all your communications.

SOME OPTIONS

Signal provides the most extensive privacy protections through its use of end-to-end encryption, and it's available for download across the globe.

Meta's WhatsApp and Facebook Messenger use end-to-end encryption, but collect more metadata than Signal (and Messenger doesn't use end-to-end encryption in group chats).

Apple's FaceTime and iMessage provide end-to-end encryption in its chats.

WANT MORE INFORMATION?

Read EFF's guide to Communicating With Others Online at **https://ssd.eff.org/module/communicating-others**

TAKE BACK CTRL

WHEN POSTING ON SOCIAL MEDIA

Depending on your circumstances, you may need to protect yourself against the social network itself, against other users of the site, or both.

WHEN CREATING AND USING YOUR ACCOUNTS

Talk with your friends about the potentially sensitive data you reveal about one another online, such as your real names and personal pictures.

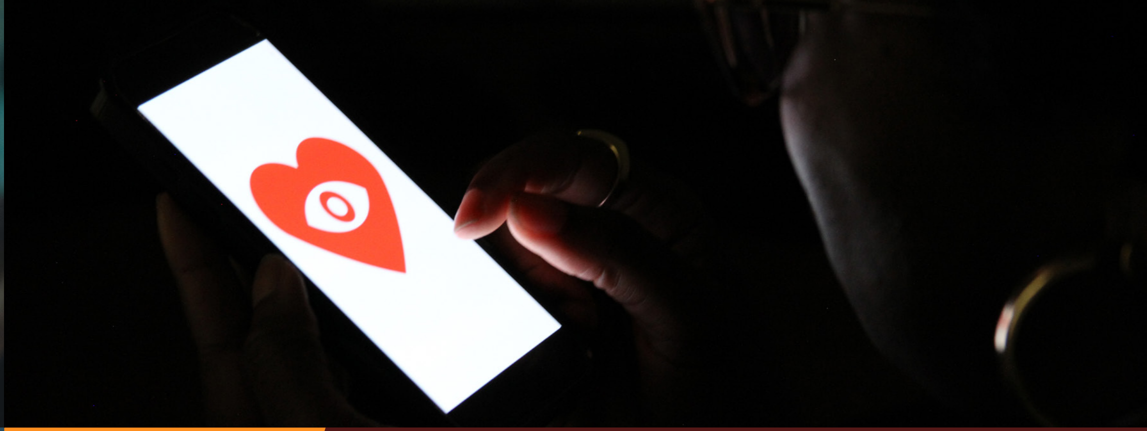
Change the default settings. Do you want to share your posts with the public, or only with a specific group of people? Should people be able to find you using your email address?

Turn off app access to location, pictures, contacts, and anything else that isn't absolutely necessary for the app to function.

Beware of password recovery questions like "What city were you born in?" as others, including law enforcement, may be able to find out these answers from your social media posts.

WANT MORE INFORMATION?

Read EFF's Guide to Protecting Yourself on Social Networks
https://ssd.eff.org/module/protecting-yourself-social-networks



TAKE BACK CTRL

WHEN ONLINE DATING

There isn't one way to use dating apps, but some small steps can prove essential in ensuring that you don't have to give up your privacy to find love:

Review your login information and use a strong, unique password for your accounts. Enable two-factor authentication when you can.

Disable behavioral ads to avoid being tracked and targeted based on your supposed interests and identities, including your sexual orientation.

Review your location, camera roll, & third-party app permissions. We recommend only enabling access to your location when you use the app, and only your general location rather than "precise location."

Consider what photos you upload and share, and assume that everything could be made public. Scrub metadata on photos by uploading screenshots instead of original pictures.

WANT MORE INFORMATION?

Watch EFF's video about dating safely online on our Instagram and TikTok accounts:
https://instagram.com/efforg
https://tiktok.com/@efforg

TAKE BACK CTRL

WHEN ATTENDING PROTESTS

There are risks associated with attending a protest, and taking steps to mitigate them can go a long way in ensuring you—and the information you value—stay safe.

PROTECT YOUR DATA

Avoid biometrics. Use a strong lock screen passcode and remove fingerprint unlock and Face ID.

Back up & encrypt. Enable full disk encryption on your device; and back up the data on your phone as it might be damaged, stolen, compromised, or lost.

Cover any identifiable features & wear nondescript clothing to avoid being identified by face and tattoo recognition technologies.

Be mindful of what you post before, during, and after protests as police can often access social media posts.
Blur out the faces and identifying marks of protestors.

PROTECT YOUR LOCATION

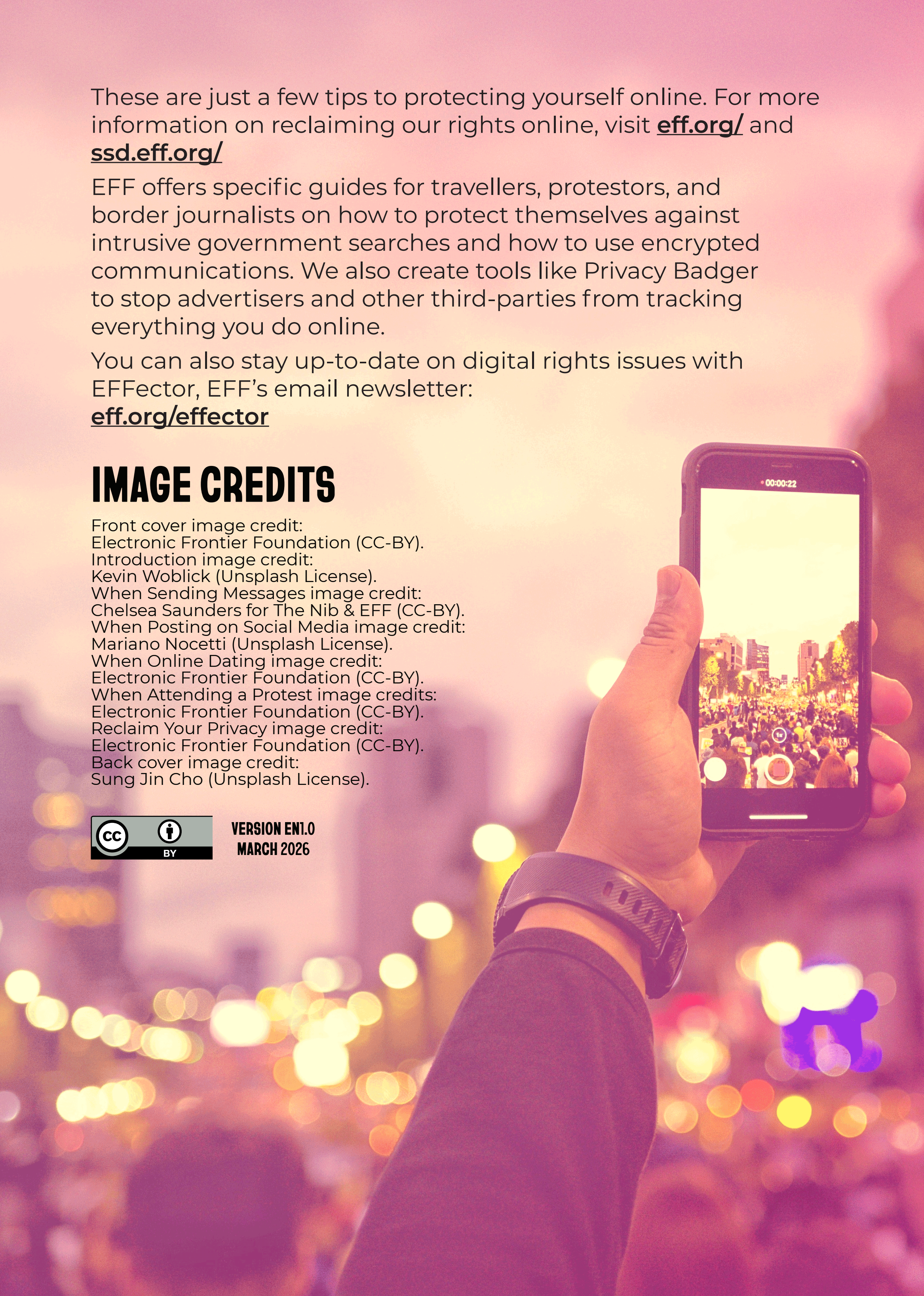
Enable Airplane mode & turn off location services to reduce the risk of app companies collecting your location and sharing with third parties like governments.

Download area maps and arrange meeting spots with friends ahead of time.

Consider biking, walking, or taking public transportation to avoid any license plate readers from capturing your vehicle's exact time, date, and location.

WANT MORE INFORMATION?

Read EFF's full protest guide at
https://ssd.eff.org/module/attending-protest



These are just a few tips to protecting yourself online. For more information on reclaiming our rights online, visit **eff.org/** and **ssd.eff.org/**

EFF offers specific guides for travellers, protestors, and border journalists on how to protect themselves against intrusive government searches and how to use encrypted communications. We also create tools like Privacy Badger to stop advertisers and other third-parties from tracking everything you do online.

You can also stay up-to-date on digital rights issues with EFFector, EFF's email newsletter:
eff.org/effector

IMAGE CREDITS

Front cover image credit:
Electronic Frontier Foundation (CC-BY).
Introduction image credit:
Kevin Woblick (Unsplash License).
When Sending Messages image credit:
Chelsea Saunders for The Nib & EFF (CC-BY).
When Posting on Social Media image credit:
Mariano Nocetti (Unsplash License).
When Online Dating image credit:
Electronic Frontier Foundation (CC-BY).
When Attending a Protest image credits:
Electronic Frontier Foundation (CC-BY).
Reclaim Your Privacy image credit:
Electronic Frontier Foundation (CC-BY).
Back cover image credit:
Sung Jin Cho (Unsplash License).

VERSION EN1.0
MARCH 2026