MOBILE APPS FOR NONPROFITS:

A FACT SHEET FROM THE ACLU

Mobile apps can help your organization recruit, educate, and engage people. But when your community members use mobile apps, they leave behind digital footprints about their interests, habits, and concerns. If you're thinking about jumping on the app bandwagon, take a few moments to make sure your app protects this sensitive information properly.

APP USE IS ON THE RISE

Eighty-five percent of Americans have mobile phones—with even higher ownership rates among young people (96% of 18-29 year-olds) and community members of color (87% of African Americans and English-speaking Latinos)—and mobile users spend more time using apps than surfing the Web. That's why apps are such an appealing way to reach your members.

BUT PERSONAL INFORMATION SHOULD NOT BE THE PRIZE

Many apps need some information in order to work, but far too many of them are collecting, retaining, or sharing unnecessary data—such as location information—when they don't need to. And just because it's "your" app doesn't mean you're the only ones who could access this information. A security breach or legal demand could expose data that you hold yourself. In addition, app developers, platform providers (like Apple for iPhone apps) and cell carriers, and analytic services could all possibly access—or reveal—your users' personal information. It's up to you to make sure that your users' personal data is used properly.

ACT NOW TO PROTECT YOUR APP USERS – LEARN HOW YOU CAN HELP

1. **Know your app.** Talk to your app developer before work begins and make sure that you understand exactly what kind of data your app will collect, retain, and share, and why this data is necessary. Ensure that your app doesn't collect more data than it needs.
2. **Protect user information.** Insist that any information your app collects—on the phone or in a remote database—is held as securely as possible, and that your app regularly delete data that is no longer necessary.
3. **Test drive your app.** Before you release and promote your app, test it and be certain it works as planned. Enlist an expert if necessary to make sure the app is secure.
4. **Put your users in control.** Your app should give users control over their personal data. Provide notice explaining the information the app will capture and how it will be used, allow users to decline to share certain data, and make it easy for users to view and correct their own information and to remove the app entirely.
5. **Demand a privacy upgrade.** Outdated privacy laws, written before the Web existed, allow the government to try to get its hands on the treasure trove of sensitive information collected by your app. Join us in working to update privacy laws and demand that companies incorporate stronger privacy protections. It's time to Demand our dotRights!

LEARN MORE AT DOTRIGHTS.ORG
OR FIND US ON FACEBOOK OR TWITTER AT @DOTRIGHTS

ACLU
AMERICAN CIVIL LIBERTIES UNION of NORTHERN CALIFORNIA

WWW.DOTRIGHTS.ORG

DEMAND YOUR dotRIGHTS