MARKETING YOUR MOBILE APP

GET IT RIGHT FROM THE START

FEDERAL TRADE COMMISSION | business.ftc.gov

CONGRATULATIONS! The app business is growing rapidly and you've decided to get in on the boom. Maybe you work for an exciting start-up or are striking out on your own. Regardless of the size of your business, the Federal Trade Commission (FTC)—the nation's consumer protection agency—has guidelines to help you comply with truth-in-advertising standards and basic privacy principles.

"But we're a small company and haven't made any money from our app yet." All the more reason to build compliance in from the start. Laws that apply to established businesses apply to you, too, and violations can be costly. In addition, satisfied users may be your best form of marketing. Breaking into the business with an app that delivers on its promises is key to your long-term success.

Of course, there's no one-size-fits-all approach. Every app is different. Still, there are some general guidelines that all app developers should consider.

TRUTHFUL ADVERTISING

TELL THE TRUTH ABOUT WHAT YOUR APP CAN DO.

Once you start distributing your app, you become an advertiser. Under the law, an ad isn't just a multimillion dollar TV campaign. It's pretty much anything a company tells a prospective buyer or user – expressly or by implication – about what a product or service can do. Whether it's what you say on a website, in an app store, or within the app itself, you have to tell the truth. False or misleading claims, as well as the omission of certain important information, can tick off users and land you in legal hot water. One rule of thumb: Look at your product and your advertising from the perspective of average users, not just software engineers or app experts. If you make objective claims about your app, you need solid proof to back them up before

you start selling. The law calls that "competent and reliable evidence." If you say your app provides benefits related to health, safety, or performance, you may need competent and reliable *scientific* evidence. For example, the FTC has taken action against developers who said their apps could treat acne and developers who said their apps could diagnose melanoma risk, but who didn't have scientific evidence to back up their claims. Visit the BCP Business Center at business.ftc.gov for more on keeping your claims compliant.

DISCLOSE KEY INFORMATION CLEARLY AND CONSPICUOUSLY. If you need to disclose information to make what you say accurate, your disclosures have to be "clear and conspicuous." What does that mean? That they're big enough and worded clearly so users actually notice them and understand what they say. Generally, the law doesn't dictate a specific font or type size, but the FTC has taken action against companies that have buried important terms and conditions in long licensing agreements, in dense blocks of legal terms, or behind vague hyperlinks. Clear and conspicuous disclosures make good business sense. Most people react negatively if they think a company is trying to pull a fast one by hiding important information. Users are more likely to continue to do business with a company that is straight forward.

PRIVACY AND DATA SECURITY

BUILD PRIVACY CONSIDERATIONS IN FROM THE START. The FTC calls this "privacy by design." What does it mean? Incorporating privacy protections into your practices, limiting the information you collect, securely storing what you keep, and safely disposing of what you no longer need. Apply these principles in selecting the

default settings for your app and make the default settings consistent with what people would expect based on the kind of app you're selling. For any collection or sharing of information that's not apparent, get users' express agreement. That way your customers aren't unwittingly disclosing information they didn't mean to share.

BE TRANSPARENT ABOUT YOUR DATA PRACTICES. Even if you need to collect or share data so your app can operate, be clear to users about your practices. Explain what information your app collects from users or their devices and what you do with their data. For example, if you share information with another company, tell your users and give them information about that company's data practices.

OFFER CHOICES THAT ARE EASY TO FIND AND EASY TO USE. Give your users tools that offer choices in how to use your app—like privacy settings, opt-outs, or other ways for users to control how their personal information is collected and shared. It's good business to apply the "clear and conspicuous" standard to these choice mechanisms, too. Make it easy for people to find the tools you offer, design them so they're simple to use, and follow through by honoring the choices users make.

HONOR YOUR PRIVACY PROMISES. "But we don't make any promises." Think again and reread your privacy policy or what you say about your privacy settings. Chances are you make assurances to users about the security standards you apply or what you do with their personal information. At minimum, app developers—like all other marketers—have to live up to those promises. The FTC has taken action against dozens of companies that claimed to safeguard the privacy or security of users' information, but didn't live up to their promises in the day-to-day operation of their business. The FTC also has taken action against

businesses that made broad statements about their privacy practices, but then failed to disclose the extent to which they collected or shared information with others—like advertisers or other app developers. What if you decide down the road to change your privacy practices? You'll need to get users' affirmative permission for material changes. Just editing the language in your privacy policy isn't enough in those circumstances. And while you're taking another look at your privacy promises, read them with users in mind. Is the language clear? Is it easy to read on a small screen? Are you using design elements—color, fonts, location, and the like—to call attention to important information?

PROTECT KIDS' PRIVACY. If your app is designed for children under 13 and collects personal information, you have additional requirements under the Children's Online Privacy Protection Act (COPPA) and the FTC's COPPA Rule. But COPPA compliance doesn't end there. Regardless of the kind of app you sell, if you know you're collecting personal information from children under 13—or if you know you're collecting personal information from another website or online service (including another app) that's designed for kids under 13—COPPA applies.

What does COPPA require? Under COPPA, you have to clearly explain your information practices, provide direct notice to parents about those practices, and get parental consent before collecting personal information from kids. These obligations apply to you when third parties (like ad networks or plug-ins) collect personal information through your app. COPPA also requires that you keep "personal information" collected from children confidential and secure. The rule defines "personal information" to include a first and last name, an address, a telephone number, online contact information, a screen name or user name that functions

like online contact information, geolocation information, or a persistent identifier that can be used to recognize a user over time and across different websites or online services (such as device identifier, cookie, serial number, or IP address). Visit the FTC's COPPA site at ftc.gov/coppa for compliance advice.

COLLECT SENSITIVE INFORMATION ONLY WITH CONSENT. Even when you're not dealing with kids' information, it's important to get users' affirmative OK before you collect any sensitive data from them, like medical, financial, or precise geolocation information. It's a mistake to assume they won't mind.

KEEP USER DATA SECURE. At minimum, you have to live up to the privacy promises you make. But what if you don't say anything specific about what you do with users' information? Under the law, you still have to take reasonable steps to keep sensitive data secure. One way to make that task easier: If you don't have a specific need for the information, don't collect it in the first place. The wisest policy is to:

1. collect only the data you need;
2. secure the data you keep by taking reasonable precautions against well-known security risks;
3. limit access to a need-to-know basis; and
4. safely dispose of data you no longer need.

These principles apply both to information you ask users to give you and to any information your software collects. If you work with contractors, make sure they abide by the same standards. The FTC has free resources to help you develop a security plan appropriate for your business. One place to start: Protecting Personal Information: A Guide for Business at ftc.gov/protectingpersonalinfo.

ABOUT THE FTC

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace. The Business Center gives you and your business tools to understand and comply with the law. Regardless of the size of your organization or the industry you're in, knowing – and fulfilling – your compliance responsibilities is smart, sound business. Visit the Business Center at **business.ftc.gov**

YOUR OPPORTUNITY TO COMMENT

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to **sba.gov/ombudsman**.

Federal Trade Commission
BCP Business Center

business.ftc.gov
September 2020