



Getting Smart About Smartphones: *Tips for Consumers*

Consumer Information Sheet 15A • December 2014

Our phones have become pocket computers. Think of the information your smartphone holds: call logs, text messages, your location, your contacts, photos, videos, and your web browsing history. Think of what it can do: stream movies, hail a cab, make purchases, and talk to you, among other things.

If, like many Americans, you say your life is in your phone, then it's time to get smart about how you use it. Your safety depends on it.

Smartphone Risks: Reality Check

Smartphones (and tablets and other portable devices that can access the Internet) bring privacy risks, like their desktop counterparts. They can be targets for malware and spyware and vulnerable to hackers. Even so, many consumers do not protect their phones with security software – or even with a passcode.

Smartphones hold very personal information that we want to keep private, such as text messages, photos, and our friends' contact information. If you use your phone for online banking, your account password may be stored on the phone. And some of the apps that make our phones so useful have been found to capture a wide range of our personal information.

Smartphone Privacy: Own it

Your privacy may be at risk even if you keep your phone with you at all times. Avoid complacency and take steps to protect yourself today. See the basic tips below and then go to the For More Information section at the end of this sheet for additional resources.

First, Secure Yourself

In public places, be alert when using your phone: smartphones are valuable. Criminals snatch phones from distracted texters and talkers, frequently hurting the victims. Stolen smartphones not only have value on the resale market, they are also valuable to identity thieves who use stored personal information to commit crimes.

In the driver's seat, turn off your phone. If you need to make a call or send a text, pull over to do it. Powering down your smartphone when you are behind the wheel can save lives – including your own.

Secure Your Phone

- Know where your phone is at all times. Don't let people you don't know have access to it – malware, spyware, or tracking apps can be installed in just a few minutes.
- Protect your phone with a password or pin. Install security software. Make sure to keep the software updated.

- Keep your phone's operating system up to date. This will protect you with patches for newly discovered bugs or hacks.
- Use an app or a service that lets you remotely erase the information on the phone if it's lost or stolen. You must set this up in advance, before the phone goes missing.
- Back up your smartphone's contents to your computer or to mobile cloud storage. Device manufacturers and others offer mobile cloud storage.
- You can also better protect your private information by using your smartphone "settings."
- Auto-lock: Phones are small and easy to lose. Set yours to auto-lock within five minutes, with a password to unlock it.

Review Location Services

- Location services make life convenient. They are how apps on our devices deliver accurate directions, traffic updates, nearby restaurants, and weather reports. However, an app can access your location even when you are not using the app.

You don't have to make your location available all the time. Adjust your settings and control location services:

- On *Android phones and devices*, go to Settings, then Location and uncheck the boxes. When an app asks for access to your location, you can choose to grant it or not.

You can also choose how accurate you want your location reporting to be. Location can come from GPS plus WiFi and cellular networks, or just one or the other. Keep in mind that a higher degree of accuracy will use more battery, so protecting your privacy protects your battery life too.
- On *iPhones and iPads* (iOS6 and later), go to Settings, then Privacy, then Location Services. You can turn it off. Or you can

choose which functions and apps to give access to your location.

You may get notifications from apps asking to use your location in the background. For privacy, select "Don't Allow."

- On a Windows phone, you can disable all access to location information by apps and collection of your location information by the Windows Phone location service. Go to Settings, then Location, and toggle the location switch to off.
- On a BlackBerry 10, select the Settings icon on the main screen, then Location Services from list, and use Location Services toggle button to turn on/off location services.
- On a BlackBerry 7 and earlier devices, on the home screen, select Options, then Device, then Location Settings. Use the toggle switch to turn on/off location services and GPS assistance.

Check Your Network

- Be careful about banking where you buy your latte. Free public Wi-Fi is normally not secure, and information thieves know it. They sit in cafes, shopping malls, and other public places monitoring how you use the Internet. Your passwords, account numbers, and photos can fall prey to hacking. When using Wi-Fi hot spots, stick to window-shopping.

Check Out Apps

Over a million mobile apps are available today. They let us do many wonderful and useful things. They can also access our personal information and even our phone's functions. Pause a moment and check out the features of the latest cool app before you download it.

- In the app platform/store, look for a link to the app's privacy policy. Look through the policy for what it says about personal

information they collect and how they use and share it. If you don't like what you see, don't download the app.

- On Android phones, the Permissions tab on app pages in GooglePlay store displays the information and features that the app can access on your phone. For example, it may show that an app can make phone calls and incur charges. If you don't like the permissions, don't download the app.
- Once you've downloaded an app, pay attention to any notices asking for your permission to access your location or other information.
- Look for a privacy policy and privacy settings within the app after you've downloaded it. You may be able to make choices about what information an app collects or how it uses it.
- California law requires apps to have a privacy policy.¹ If you can't find an app's privacy policy, or if you have a complaint about the app's privacy practices, report it.
 - For apps in the Microsoft Windows store: Look for a link labeled "Report app to Microsoft" or "Report concern to Microsoft."
 - For apps in the Apple AppStore: Go to www.apple.com/privacy/contact/.
 - For apps in GooglePlay: Visit the app's description page to "Flag as inappropriate"

or go to <https://support.google.com/googleplay/android-developer/contact/takedown>.

- For apps in BlackBerry World: Send an email to privacyoffice@rim.com.
- Report to the California Attorney General: www.oag.ca.gov/contact/consumer-complaint-against-business-or-company

For More Information

App Reviews, Common Sense Media, available at www.commonsensemedia.org/app-reviews

"How to clear your data off a device," Computerworld (August 2012), available at http://www.computerworld.com/s/article/9229969/How_to_clear_your_data_off_a_device

"Before It's Gone: Steps to Deter Smartphone Thefts & Protect Personal Info," CTIA (the wireless association), available at www.ctia.org/consumer_info/index.cfm/AID/12084.

"The Best Mobile Security Apps," PC Magazine (May 2012), available at www.pcmag.com/article2/0,2817,2402099,00.asp

"How to Remotely Disable Your Lost or Stolen Phone," PC Magazine (April 2012), available at <http://www.pcmag.com/article2/0,2817,2352755,00.asp>.

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice on a particular case, you should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the California Department of Justice, and (3) all copies are distributed free of charge.

NOTES

¹ The California Online Privacy Protection Act, Business and Professions Code §§ 22575-22579.