Published on *Privacy Rights Clearinghouse* (https://www.privacyrights.org)

Home > Smartphone Privacy

Smartphone Privacy [1]

Posted Aug 01 2005
Revised Dec 19 2017

1. Introduction

Smartphones allow us to communicate via talk, text and video; access personal and work e-mail and the Internet; run applications; make purchases; manage bank accounts; take pictures - and for many of us are an integral part of our everyday lives. Essentially tiny computers, we reach for these devices when we first wake up, bring them with us into the car, and often keep them with us during our most private moments.

Clunky, expensive versions of smartphones have been around since as early as 1992, but it wasn't until Apple released the iPhone in 2007 that smartphones reached the mass market. According to a January 2017 Pew Internet Report [2], 77% of American adults have a smartphone. While they provide us with seemingly unlimited amounts of useful tools, most of us don't consider the massive amount of personal data we carry around in (and is collected by) our smartphones.

Unlike many computers and other devices, our smartphones are always with us and many of us rarely turn them off. Despite the amount we use them and the dependence we place on our smartphones, the Pew Internet Center reported in January 2017 [3] that more than a quarter of smartphone users surveyed – 28% - do not use any form of screen lock to secure their phones, and one in ten never update their phones or applications! In this guide, we explain the privacy implications of smartphones and offer practical tips to help you protect your privacy.

2. What is your smartphone capable of revealing about you?

It's safe to assume that anything you do on your smartphone and any information you store is at risk of being snooped on or inadvertently given away if you don't take proper precautions. What is *everything*? Well, consider your personal conversations via text, email, or instant messenger app; any online accounts and passwords you may type into your phone; your contacts and call history; your location data and history; your web browser history; and your photos, videos, snaps, swipes and matches. It's hard to overstate how much of our personal lives we can potentially reveal to our smartphones.

3. Who may have access to the information your smartphone collects and stores?

You can think of your smartphone as a network of connected services, each of which may offer some access to information stored or collected on your phone. Your phone receives internet and telephone service from an internet service provider. Your phone's operating system may collect usage data and transmit it back to its developers. Applications running on your phone may be granted access to certain sensors or data, and may be sharing that data with the developer (and advertisers). Criminals may infiltrate your phone through malware, hacking, or physical access to your device. In some cases, government may be very interested in accessing information on your phone. By knowing what services may be able to collect data through your smartphone, you can make more informed decisions to better protect your privacy.

a. Service providers

When exploring what your smartphone says about you, it's useful to begin at the service provider – the company that provides the cellphone service and internet connection to your device. Service providers (like AT&T, Sprint, Verizon, and T-Mobile) collect data, but are not always forthcoming in detailing exactly what data they collect, the reasons they collect it, and their data retention policies. At the very least (and, unavoidably), smartphone service providers collect the following:

- Incoming and outgoing calls: the phone numbers you call, the numbers that you receive calls from, and the duration of the call;
- Incoming and outgoing text messages: the phone numbers you send texts to and receive texts from;
- How often you check your e-mail or access the Internet;
- Your general location: by cell tower (to be distinguished from your precise location gathered by sensors in your device).

Data retention policies – or how long the various services keep records of the information they collect - vary among service providers, and certain records are kept longer than others.

Privacy tip: find your service provider's privacy policy and opt out of sharing when possible

Unfortunately, there is little you can do about the data your service provider collects, but you may be able to stop the data from being shared with third parties such as advertisers. Some service providers offer a way to opt out of certain types of data use. Either contact your cell phone service provider or look at its privacy policy online to find out what it shares with third parties and whether you can opt out of the sharing.

- **Verizon**: Go to www.verizon.com/privacy [4] to read the privacy policy or e-mail privacyoffice@verizon.com [5]. Verizon allows its customers to opt-out of certain advertising and marketing programs by following the instructions here [6] (though if you'd like to opt out of advertising services over the internet you will need to log in using a Verizon account) or by calling Verizon at 1-866-211-0874.
- **T-Mobile**: T-Mobile's privacy policy can be found at https://www.t-mobile.com/company/website/privacypolicy.aspx#fullpolicy [7], and, as with most service providers, T-Mobile uses your internet and browser history to serve "interest-based advertising" to its customers. You can, however, opt out of this type of advertising by clicking here [8] from your T-Mobile device, or by visiting www.aboutads.info/choices [9] from your computer or non-mobile device.

T-Mobile also allows customers to manage their preferences for marketing communications by logging into the my.t-mobile.com [10] profile, by contacting Customer Service by dialing 611 from a T-Mobile phone, or 1-844-351-4197, through e-mail at privacy@t-mobile.com [11], or by writing to:

T-Mobile USA, Inc.
Attn: Chief Privacy Officer
12920 SE 38th Street
Bellevue, WA 98006

- **AT&T**: AT&T's privacy policy can be found at http://about.att.com/sites/privacy_policy [12] , along with a simplified summary of the policy and frequently asked questions. AT&T does not allow users to opt out of "first party" advertising – or advertising for AT&T services and products, but does give some amount of choice in how your data is shared with third party advertisers. You can find information about how to opt out of various types of advertising online by following the advice of the *Your Choices and Controls* section of the privacy policy, here. [13]

  You can email AT&T's privacy office at privacypolicy@ATT.com [14], or write to:

AT&T Privacy Policy
Chief Privacy Office,
208 S. Akard, Room 1825
Dallas, TX 75202

AT&T is also a member of the TRUSTe Privacy Seal Program which allows consumers to file privacy complaints [15].

- **Sprint**: Go to www.sprint.com/legal/privacy.html [16] to read the privacy policy. Sprint offers opt-in advertising, meaning that users are not signed up for the service by default. You can find more information about their advertising program here [17], but according to their policy, unless a customer opts in to such a service, Sprint will not use, or allow its ad partners to use, information Sprint collects about the websites you visit or the applications you use in order to target advertising at you. If you have opted in to the service, you can opt out by calling 1-855-596-2397, or visiting http://www.sprint.com/mychoices [18] If you have questions about the policy, e-mail officeofprivacy@sprint.com [19], or write to:

  Sprint Nextel Office of Privacy-Legal Department
  P.O. Box 4600
  Reston, VA 20195

  Privacy tip: Scan the privacy policy for important information

For most of us, the idea of reading a privacy policy and actually understanding its implications can be a challenge. Keep in mind that privacy policies aren't necessarily written to clearly inform you of a company's privacy practices, but rather to disclaim liability. However, there are a few tips you can follow to get the most useful information out of any privacy policy:

- Look for sections about control or choice over your information. *My Choices* or *Your Rights and Choices* are the types of section headers to look for.
- Look for a point of contact. Almost every privacy policy will contain information describing how to contact the company to ask questions and exercise out-out choices.
- Read the California Attorney General's guide on reading and understanding privacy policies [20] for more detailed information.

  Privacy tip: Minimize the information you leak to service providers by changing how you use your smartphone

For example, knowing that your provider is always able to see text messages, you may choose to limit the number of text messages you send by using a dedicated messaging application such as WhatsApp or Signal. Similarly, voice-over-internet applications such as Skype, Google Hangouts, or Apple's FaceTime will not leak the same caller information (to your service provider, at least) that is transmitted when placing a telephone call. Placing a call or sending a text message is often unavoidable, but by switching to secure messaging applications for communications with your closest network of family or friends you can dramatically limit the exposure of some of your most personal information to service providers.

Both iPhone and Android smartphones allow you to toggle whether your cellular data is enabled. This feature is generally a bandwidth-saving tool rather than a privacy-focused one. As a result, toggling cellular data connection frequently only toggles off cellular *data* and not cellular *voice*. For example, connecting through Wi-Fi with cellular data turned off will hide the internet traffic that could leak to your provider, but it might not hide the location information from the cell tower the phone is connecting through to receive telephone services. If you are concerned about your service provider having access to the location or telephone information from your smartphone, instead enable *Airplane Mode* on your device to completely toggle the cellular radio off.

b. Advertisers

Advertisers want to market to the people who are most likely to buy their product or service. The more information they collect about you, the better their ability to know the types of products and services you are most likely to buy. One privacy concern here is that information could be shared with third parties and compiled with other data to create a detailed profile about you without your knowledge or consent.

i. Personal information collected by apps

People are increasingly spending more time using mobile applications than they are browsing the mobile web. There are literally millions of apps available for your mobile devices, and anyone can create an app. The app marketplace is filled with numerous free or low-priced choices. Apps can collect data using any of the device sensors authorized through the phone’s permissions, and transmit it to the app maker and/or third-party advertisers. It can then be shared or sold.

Advertisers pay app developers to get access to you. The advertisers supply code to the app makers to build into the app. The code not only makes an ad appear when you use the app, but also collects data from your phone and transmits it back to the advertiser. It's also possible that the app itself collects data [21] which is shared with ad networks. The ad networks may then show the user ads that contain content based on the data collected. The data collected and/or shared can be used to build a detailed profile about you, re-packaged and sold to the highest bidder.

Even an app as seemingly harmless as a flashlight, game, or radio might collect such information as your device ID, your contacts and/or your location. Examples such as the *Brightest Flashlight* app [21], which was downloaded more than 50 million times and had an average five-star rating on the Google Play Store, illustrate how risky the smartphone app market can be, and how difficult it can be for users to be safe and secure with their smartphone applications. Unfortunately, even users that are following best practices could have been tricked into downloading this app; which shared user location and device identification information with third-party advertisers.

In fact, the Internet Advertising Revenue Report from 2017 [22] found that digital ad revenue grew 22 percent from 2016 to 2017, and for the first time, mobile ads accounted for more than half of all digital ad revenue - $36.6 billion. Perhaps unsurprisingly, the vast majority of that ad revenue is going to one of two companies: Google – which develops the Android operating system that runs on nearly 90 percent of smartphones worldwide [23] – and Facebook - the social network that counts as subscribers 72.4% of Americans [24] (and 26.3% of the world). According to research published in Scientific American in 2017 [25], 70% of smartphone apps share your data with third-party services.

Who makes these apps, what data do they collect, how do they store your data, and where is your data going? These are the questions you should be asking. You may be able to find the answers in the app's privacy policy.

The Federal Trade Commission's guide *Marketing Your Mobile App: Get It Right from the Start* [26] helps mobile application developers observe truth-in-advertising and basic privacy principles when marketing new apps.

ii. Personal information collected from behavioral marketing or targeting

Behavioral marketing or targeting refers to the practice of collecting and compiling a record of individuals' activities, interests, preferences, and/or location over time. This data may be compiled, analyzed, and combined with information from offline sources to create even more detailed profiles.

Marketers can then use this information to serve advertisements to an individual based on his or her behavioral record. For example, ads may be displayed based on where a person is located or the types of apps they've expressed an interest in. Advertisers believe that this may help them deliver their mobile advertisements to the users who are most likely to be influenced by them.

Some mobile browsers support the use of third-party cookies which may be used by ad networks to enable tracking. Cookie settings in your smartphone's browser allow you to remove these cookies. However, mobile apps generally do not provide ad networks with the ability to set a cookie to track users. Instead, ad networks may use your smartphone's device identifier. To opt-out of targeting that relies on your smartphone's device identifier, you must provide the ad networks with your identifier to be kept on their "do not target" list. You can learn how to do this by reading Expressing Your Behavioral Advertising Choices on a Mobile Device [27].

Privacy tips for downloading and using apps safely and securely

- Research apps before you download. Look at how many people have downloaded the app, read what they have said about it, and determine who created it. In some cases, an app may replicate features that are available through a service's website. If that is the case, you may want to consider accessing the service through your smartphone's web browser.
- Look for a privacy policy. If the app store or download screen doesn't show it, usually the app's website will.
- Ask yourself whether the app requests access to information you are uncomfortable with. There can be very good reasons for certain applications to be requesting permissions [28] that seem broader than necessary at first glance, but a general rule is to avoid applications that request more permissions than seems necessary for the service it provides. Learn where to go on your particular phone to determine what you will allow the app to access, and if you are at all suspicious do more research on the app before you download. If you are using an Android phone, the install screen will give you details about what data it will access. Unfortunately, iPhone apps don't indicate which permissions will be needed at the install screen, but you can see which apps want to access your location or other services by going to Settings > Privacy [29]. If you are not using Android or iOS (though that is unlikely: Android and iOS accounted for 99.6 percent of all smartphone sales in the fourth quarter of 2016). [30] research your particular operating system to educate yourself on this practice.

iii. Wearables and connected devices

Wearables and connected devices present many of the same privacy issues as smartphones. Unfortunately they are frequently even less secure, receive even fewer software updates, are cheaper to manufacture and can be just as (if not more) invasive into your personal life.

The *Internet of Things* is the network of internet-connected devices in homes, cars, and on our persons that promises to bring the convenience and utility of our computers and smartphones to everything around us. These devices open the door to home automation and consumer-focused artificial intelligence, but are also (like smartphones) a network of connected services and sensors. They are almost exclusively controlled by a connected application on an iOS or Android smartphone.

In addition to the privacy and security risks arising from a poorly secured or manufactured devices, developers and manufacturers of connected devices may share some of the data collected with third parties such as advertisers. In the case of wearable health and fitness devices, this data may include heart rate, pulse, exercise data, geo-location information associated with workout routines, sleep data, personal hygiene patterns, dietary preferences, or any number of extremely revealing personal information.

Many individuals mistakenly believe that personal information collected by wearables or health and fitness devices is protected by health privacy laws like HIPAA. In reality, most if not all of that data can be freely contracted away through a device's Terms of Use. Read the privacy policy associated with the device or the company that manufactures your wearable, and see how they treat data that is collected by the device, who they share it with, and under what circumstances. You should be able to see if you have any choice in the matter, and if you don't, consider whether you actually need the device at all.

If you do decide to connect wearable devices to your smartphone, consider only connecting the devices when necessary and keeping Bluetooth turned off on your phone whenever possible. Ideally you should configure your home router so that any items that need to connect to the Internet connect to a separate Wi-Fi network than your primary network. As you connect more devices, it's a good idea to keep an eye on the total number of connected services. All too frequently these devices remain in use long after they stop receiving security updates. Try to disconnect any Internet of Things or wearable devices that you are no longer using.

c. Law enforcement

The ability to collect data on where a person has gone and what they have been doing is valuable information for law enforcement. If you are the subject of an investigation or even if you have just been pulled over, police may want to see what you've been doing and where you've been going – things your smartphone may be able to reveal. The Supreme Court has recognized that smartphones pose a unique privacy concern. Law enforcement officers must have a search warrant before they can search the contents of a smartphone.

Law enforcement has also been known to tap into the locations of smartphones, ask wireless providers to turn over troves of location data, pay third parties to unlock smartphones, and implant tracking devices. They may also request data your smartphone provider has collected about you, and can subpoena any of the intermediary service providers or connected services for any information that you've authorized them to collect. Federal privacy laws have not kept up with the pace of technology and courts are unclear on how easy it should be for law enforcement to gain access to your smartphone and its data.

For more information, see the ACLU's site on surveillance [31] and the EFF's resources on NSA Spying [32]

d. Criminals

Your service provider, advertisers, and government aren't the only parties potentially gleaning information about you from your smartphone. A cybercriminal may want to: steal money, collect personal data to commit identity theft, or engage in harassment. To further their goals, cybercriminals may try to steal your phone or find ways to use your smartphone to snoop on you through malware or public Wi-Fi networks.

i. Theft

Smartphones store a tremendous amount of personal information. If your smartphone were lost or stolen, what information would someone be able to access? Obviously it depends on how you use your phone, but assuming that the criminal could get past the password lock on your lock-screen, at the very least they would have access to your contacts list, your messages, your browser history, your connected accounts (social media, banking apps, email accounts, etc.), your photos and videos on the device, and anything else that would be available offline on your phone. If you allow your web browser to remember usernames and passwords for forms online, you might also be giving a criminal access to any accounts that you regularly log in to from your phone. Ultimately, physical access to the device gives the criminal some of the most thorough and complete access to the data available on your smartphone, and as such, it's vitally important to take some steps to secure your phone in the eventuality of a theft.

Privacy tips: Avoid and mitigate risks of smartphone theft

- Never leave your phone unattended.
- Password protect your phone with a strong password. Try to avoid simple, short numerical, or pattern passcodes in favor of longer, alpha-numeric passcodes. You can usually find the feature allowing you to set a password in the phone settings. (In Android [33], open your Settings app and tap "Security & Location"; on iPhone [34], go to Settings, and select "Touch ID & Passcode".)
- Many smartphones allow the use of biometrics, such as thumbprint or facial scanning technologies, to secure the phone and unlock the screen. While these security measures are great when properly implemented, a thumb print scan should not *replace* a strong lock-screen password, and instead, should supplement it. Generally, smartphones with biometric locks require that a passcode be manually entered whenever the phone powers on, but subsequent unlocks can be made with the biometric identifier. Best practices dictate that you use a strong password *and* a biometric scan for the best combination of security and usability.
- Do not allow your smartphone to automatically remember login passwords for access to email, VPN, and other accounts. Instead, use a password manager [35] to securely store your account passwords and usernames. That way, even if your phone is stolen, criminals won't have access to your accounts simply by opening up your phone's web browser and looking into the browser history.
- Use your phone's security lockout feature. Set the phone to automatically lock after a certain amount of time not in use. Especially in cases where you use biometrics to unlock your phone, know how you can quickly set your device to require the input of a strong password manually. For example, as of iOS 11, Apple iPhones include an *Emergency SOS feature* [36] to quickly lock out your phone, send a call for help, and alert your emergency contacts by pressing the power button five times in short succession.
- Consider installing security software that allows you to remotely track, lock your phone and wipe the data. Both Apple iPhones and Google Android phones include some kind of "Find My Phone" feature that can be enabled. While this feature can be invaluable in the event that your phone is lost or stolen, it's also important to keep in mind that these features can be an avenue for attack. Features such as these allow anyone with your Apple or Google credentials to log in to a web portal and remotely track, disable or wipe your device. So before you enable remote lock features, make sure that you've followed best practices for password and account security. In cases of domestic abuse or situations where your attacker may have access to your login credentials, you may be protecting your privacy better by disabling these features, at least until you can regain control of the underlying accounts.
- Encrypt your device. If your phone *is* stolen, encrypting the phone can help to ensure that the data on the device is inaccessible to whoever has physical access to the device. Apple iPhones are encrypted by default. You can find the option to encrypt Android phones by navigating to Settings and then to Security. [37]

ii. Malware and spyware

Malware refers to all categories of malicious software, and poses a threat to your smartphone just as it does to your computer. The term "malware" includes viruses, spyware, ransomware, trojan horses, worms, and basically any other harmful software or program. The apps on your smartphone are a common avenue for transmitting malware. However, malware may also be distributed through advertising and upgrade attacks, by exploiting vulnerabilities in the operating system itself, by having physical access to the device, or even by the manufacturer [38].

Unfortunately, mobile malware attacks are on the rise [39]. This rise can be attributed in part to the fact that individuals are less likely to guard their smartphones the way they do their computers. But it's also due to the appeal of smartphones as a potential target, the proliferation of infected applications in smartphone app stores, and the rise of cheap, consumer-focused spyware and ransomware. With person-to-person payment applications and mobile banking and payment options, criminals can directly profit off of their attack. Criminals can also profit by directly charging to an individual's phone bill.

Privacy tip: Pay close attention to application permissions

Smartphone manufacturers have started providing more tools to allow customers to pay closer attention to their applications' permissions. Whether it notifies the user when the application is installed or first launched, both iPhone and Android phones alert the user to the type of permissions that the application accesses. The application may need to access your contacts list to add friends, or it might need to be able to use the camera to remotely deposit a check at your bank. By keeping an eye on permissions, you can see what applications are authorized to use the various sensors on your device. You can also revoke those permissions in part or in whole in your phone settings.

HowToGeek offers a tutorial on managing permissions on Android, [40] and you can manage which applications have access to underlying iPhone services by navigating to Settings, and then Privacy. Be vigilant in checking and managing the permissions of applications on your phone. Be wary of installing an application if it requests more permissions than seems necessary, and consider toggling off some permissions that applications request, if possible.

Privacy tip: Exercise caution when installing applications

Although generally Apple's App Store is moderated more thoroughly than Google's Play Store to prevent users from inadvertently downloading malware, malware *is* present on all the major app stores. Whenever you download an app, research the application beforehand. Read reviews and look at the total downloads. Avoid downloading applications with few reviews or downloads, and if possible, avoid downloading an application if you can accomplish the same thing through the phone's web browser. If you've downloaded an application in the past and find that you no longer use it, delete it.

iii. Geotags

Depending on your settings, your smartphone and the installed applications on your phone may be using the built-in GPS capability to embed your exact location into your posts or photos. Or it might use your location to serve you advertisements or help you check in to local businesses. These services can be welcome features, but they can also lead to unwelcome, unnecessary tracking. *Location Services* can be toggled in your phone's settings. Both iPhones [41] and Android [42] phones allow the user to easily toggle when location services are enabled and to control which applications have access to location services. Both iOS and Android have implemented features to immediately notify the user that an application is requesting location information. On Android, your status bar will show a location pin icon. And on iPhone the status bar will turn blue, meaning that some application is using your phone's location services.

The process of embedding location information into photos is called *geotagging*. If you share your photos and they end up on the Internet, criminals can use the geotag to track your movements or find out where you live. Note that Facebook automatically strips out geotags, so any photos posted to Facebook do not have your location embedded in the file.

Privacy tip: Disable photo geotagging on your phone

See instructions at HowToGeek's tutorial on preventing Android from geotagging photos [43] and TechAbout's guide to do the same for iPhones and iPads. [44] Now it's easier than ever to know at a glance that your phone is pinging location services. As mentioned above, be vigilant about allowing applications to use location services and consider manually toggling location services on and off as you need them.

iv.Through public Wi-Fi networks and Bluetooth

When your smartphone uses a public Wi-Fi network to connect to the internet (for example, in an airport or coffee shop), it may be possible for others to "see" the data being transmitted by your smartphone unless the data stream is encrypted. This data could be what you are typing (such as your bank account log-in information) or it could be information being collected by an app you are using.

Similarly, when you use Bluetooth, make sure you know and trust the connection. It's also important to turn off your Bluetooth function when you are not using it, as recently vulnerabilities in Bluetooth have been discovered [45] that may leave potentially millions of devices exposed to remote attack.

Privacy tips for using Wi-Fi and Bluetooth safely

- Use public Wi-Fi networks cautiously. Do not conduct activities that use sensitive information such as mobile banking. If you do connect to a public Wi-Fi network, operate under the assumption that anything you do on that network may be monitored, and consider connecting to a VPN to ensure that your network traffic is encrypted.
- Before connecting to any network, make sure it is one you trust. Bad actors can set up fake public networks that are only used for malicious purposes. Read *Lifehacker: How to Stay Safe on Public Wi-Fi Networks* [46] to learn more.
- Ensure that your smartphone, and any applications on the device, are up-to-date. Run any software updates as soon as they are available. As security vulnerabilities are discovered, it's important to update your device so that those vulnerabilities can be patched.

v. By tricking you or exploiting your trust

Often, cybercriminals work by exploiting consumer trust and convincing them that their links, URLs, applications or files are safe. These impersonations can appear legitimate [47] and it can be very difficult to know for sure whether or not you're on a trusted log-in page. However, they may also infiltrate legitimate software, so it's important to ensure that the applications you install and run on your smartphone are up-to-date, are from trusted developers, and are not left on your device longer than necessary if you no longer use or update the software.

Privacy tips:

- When clicking on links, downloading files, and downloading apps, make sure you are aware of and trust the source. Pay close attention to URLs and the appearance of the website you are downloading from. Look for common spelling errors in the company's website, graphics that are out of place, anything that seems out of the ordinary if you frequent the website.
- Avoid downloading anything unless you were actively seeking out the download in the first place. If you receive an email or pop-up telling you that you need to download a new application or run a virus scanner you don't have, beware! You may be unwittingly exposing your device to malware.
- Use Two-Factor Authentication wherever possible. Two-Factor Authentication requires that some other authentication method be used in addition to a username and password. This second layer can be a biometric fingerprint, an automated text message or call to your phone, a physical authentication token, or can come in the form of an app on your device. Two-Factor Authentication is one of the best ways to secure your accounts against phishing and impersonation attacks, and can also ensure that someone with physical access to your device doesn't have carte blanch access to all of your connected accounts. You can find out if the service you are using offers Two-Factor Authentication by checking the website TwoFactorAuth.org [48].

4. Do individuals have legal protections?

Yes, but privacy laws have not kept pace with technology.

a. Privacy and law enforcement: the 4th Amendment to the U.S. Constitution

Your Fourth Amendment rights affect when, how, and if law enforcement can search or seize your smartphone and the data it contains. The Supreme Court recognized in *Riley v. California* [49] that smartphones represent unique privacy concerns over traditional mobile phones, and that searching the contents of a smartphone requires a search warrant. We urge you to become familiar with the work of the American Civil Liberties Union [50], Electronic Frontier Foundation [51], and the Electronic Privacy Information Center [52] for more information.

b. Federal law

i. The Electronic Communications Privacy Act (ECPA)

Enacted in 1986, The Electronic Communications Privacy Act (ECPA) (18 U.S.C. §§ 2510-3127) includes the Wiretap Act, Stored Communications Act, and the Pen Register Act. It can apply to both law enforcement agencies and companies. ECPA makes it unlawful under certain circumstances for someone to read or disclose the contents of an electronic communication. However, there are exceptions to ECPA, and the definition of what constitutes an electronic communication is unclear given the extensive advances in technology since its enactment.

For information on ECPA reform efforts, visit the site of the Digital Due Process coalition:

Digital Due Process: Modernizing Surveillance Laws for the Internet Age [53]**.** Digital Due Process is a coalition whose goal is to "simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public."

ii. The Computer Fraud and Abuse Act

The 1984 Computer Fraud and Abuse Act [54] was enacted to prevent unauthorized access to computers. (18 U.S.C. § 1030) Considered by many to be an overbroad law, among other things it is used in prosecuting hackers, and covers information stored on computers. It is *possible* that a court of law would consider a smartphone to be a type of computer.

iii. Children's Online Privacy Protection Act (COPPA)

The 1998 Children's Online Privacy Protection Act (COPPA) protects the privacy of children under the age of 13 by prohibiting the online collection of a child's personal information without providing notice and obtaining parental consent. COPPA also prohibits requiring that a child disclose more information than is reasonably necessary to participate in an activity online. (15 U.S.C. §§ 6501-08)

If your child has a smartphone or uses yours to go online or install and use apps, you may want to learn more about COPPA [55]. If you suspect that a site or application is not complying with COPPA you can file a complaint with the FTC [56].

To learn more about COPPA visit the Center for Digital Democracy [57]**.** CDD is a non-governmental organization with resources on digital marketing, digital health issues, digital privacy issues, and youth digital marketing.

iv. The Federal Trade Commission Act

The FTC has the authority to investigate and bring an enforcement action against an entity it believes is engaging in an unfair or deceptive act or practice. In practice, this usually means that the FTC will investigate a company that is violating its own privacy policy.

The FTC also has the ability to enforce certain specific consumer protection statutes. You can file a complaint with the FTC. The FTC does not resolve individual complaints, but such complaints may contribute to an investigation or enforcement action.

c. State and federal legislation

You can research bills being considered by Congress by visiting the official website of the Library of Congress, Thomas [58], and using its search feature. The National Conference of State Legislatures [59] also provides information on state legislation concerning privacy.

Privacy tip: Voice your opinion

Write to your Congressional representatives and state lawmakers. Share your concerns with them, and voice the importance of updating existing privacy laws in order to keep pace with changing technology.

5. Where to complain

Federal Trade Commission (FTC)
Phone: (877) 382-4357
TTY: (866) 653-4261
600 Pennsylvania Avenue, NW
Washington, DC 20580

You can also file complaints with your state Attorney General's office. For more information see the National Association of Attorneys General website [60].

6. Additional resources

To learn more about phone privacy issues and tips, visit our website here [61].

Source URL (modified on January 4, 2018): https://www.privacyrights.org/consumer-guides/smartphone-privacy

Links
[1] https://www.privacyrights.org/consumer-guides/smartphone-privacy
[2] http://www.pewinternet.org/fact-sheet/mobile/
[3] http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/
[4] http://www22.verizon.com/privacy/?CMP=DMC-CV090332

[5] mailto:privacyoffice@verizon.com
[6] http://www.verizon.com/about/privacy/full-privacy-policy#limit-section
[7] https://www.t-mobile.com/company/website/privacypolicy.aspx#fullpolicy
[8] http://iba.t-mobile.com/tmo/
[9] http://www.aboutads.info/choices
[10] https://my.t-mobile.com/
[11] mailto:privacy@t-mobile.com
[12] http://about.att.com/sites/privacy_policy
[13] http://about.att.com/sites/privacy_policy/full_privacy_policy#controls
[14] mailto:privacypolicy@ATT.com
[15] http://clicktoverify.truste.com/pvr.php?page=validate&amp;companyName=AT%26T&amp;sealid=101
[16] http://www.sprint.com/legal/privacy.html
[17] https://www.sprint.com/legal/report-analytics.html
[18] http://www.sprint.com/mychoices
[19] mailto:officeofprivacy@sprint.com
[20] http://oag.ca.gov/privacy/facts/online-privacy/privacy-policy
[21] https://www.forbes.com/sites/josephsteinberg/2013/12/06/this-flashlight-android-app-has-been-secretly-and-illegally-sharing-your-personal-data-with-advertisers/#7c6c163a11be
[22] https://techcrunch.com/2017/04/26/internet-adverising-revenue-report-2016/
[23] https://www.greenbot.com/article/3138394/android/report-nearly-90-percent-of-smartphones-worldwide-run-android.html
[24] http://www.internetworldstats.com/facebook.htm
[25] https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/
[26] http://business.ftc.gov/documents/bus81-marketing-your-mobile-app
[27] http://www.applicationprivacy.org/expressing-your-behavioral-advertising-choices-on-a-mobile-device/
[28] https://support.signal.org/hc/en-us/articles/212535858-What-are-all-these-permissions-
[29] https://support.apple.com/en-gb/HT203033
[30] https://www.theverge.com/2017/2/16/14634656/android-ios-market-share-blackberry-2016
[31] http://www.aclu.org/national-security/surveillance-privacy
[32] https://www.eff.org/nsa-spying
[33] https://support.google.com/nexus/answer/2819522?hl=en
[34] https://support.apple.com/en-us/HT204060
[35] https://www.pcmag.com/article2/0,2817,2407168,00.asp
[36] https://support.apple.com/en-us/HT208076
[37] https://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/
[38] https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html
[39] https://www.nokia.com/en_int/news/releases/2017/03/27/nokia-malware-report-reveals-new-all-time-high-in-mobile-device-infections-and-major-iot-device-security-vulnerabilities
[40] https://www.howtogeek.com/230683/how-to-manage-app-permissions-on-android-6.0/
[41] https://support.apple.com/en-us/HT207092
[42] https://support.google.com/accounts/answer/3467281?hl=en
[43] https://www.howtogeek.com/303410/how-to-prevent-android-from-geotagging-photos-with-your-location/
[44] http://www.techbout.com/turn-off-geotagging-for-photos-iphone-ipad-8738/
[45] https://www.armis.com/blueborne/
[46] https://lifehacker.com/top-10-ways-to-stay-safe-on-public-wi-fi-networks-1791800347
[47] https://www.reddit.com/r/google/comments/692cr4/new_google_docs_phishing_scam_almost_undetectable/
[48] https://twofactorauth.org/
[49] https://www.aclu.org/news/supreme-court-requires-warrant-cell-phone-searches-police
[50] http://www.aclu.org/
[51] https://www.eff.org/
[52] http://epic.org/
[53] http://digitaldueprocess.org/
[54] http://www.law.cornell.edu/uscode/18/1030.html
[55] http://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites
[56] https://www.ftccomplaintassistant.gov/
[57] http://www.centerfordigitaldemocracy.org/youth-digital-marketing
[58] http://thomas.loc.gov/home/thomas.php
[59] http://www.ncsl.org
[60] http://www.naag.org/

[61] https://www.privacyrights.org/topics/phone-privacy