Privacy in the Age of the Smartphone [1]

1. Introduction

A smartphone is a small handheld electronic device that has features of both a mobile phone and a computer. Smartphones allow us to communicate via talk, text and video; access personal and work e-mail; access the Internet; make purchases; manage bank accounts; take pictures and do many other activities. They are becoming capable of doing more and more every day.

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 June 2013 Pew Internet Report [2], 56% of American adults have a smartphone. In fact, smartphone users now outnumber traditional mobile phone users. While they provide us with seemingly unlimited amounts of useful tools, most of us don’t consider the massive amount of personal data that we carry around in our smartphones.

Unlike many of our 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, it’s safe to assume that anything you do on your smartphone and any information you store is at risk of being snooped on if you don’t take proper precautions.

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 if you don’t take proper precautions.

2.a. What Information Does Your Service Provider Collect and Store?

Service providers (like AT&T, Sprint, Verizon, and T-Mobile) collect data, but are not forthcoming in detailing exactly what data they collect, the reasons they collect it, and their data retention policies. At the very least, 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 location.

Data retention policies vary among service providers, and certain records are kept longer than others. For instance, as of September 2011, Verizon, T-Mobile, AT&T and Sprint all differ [5] when it comes to how long they store any combination of call tower history records, text message detail, text message content, IP session information, IP destination information, and bill copies.

Unfortunately, there is nothing 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 (e.g. advertisers). Some service providers offer an optout from certain types of advertising.

Consumer Privacy Tip: 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](http://www.verizon.com/privacy) [6] to read the privacy policy, call 1-866-211-0874, or e-mail [privacyoffice@verizon.com](mailto:privacyoffice@verizon.com) [7]. Verizon allows its customers to opt out of certain advertising and marketing programs [here](https://www.privacyrights.org/verizon-privacy-policy.html) [8].

Verizon is also a member of the TRUSTe Privacy Seal Program which allows consumers to file privacy complaints [9].

- **T-Mobile**: Go to [www.t-mobile.com/company/website/privacypolicy.aspx](http://www.t-mobile.com/company/website/privacypolicy.aspx) [10] to read the privacy policy, call 1-877-937-8997, e-mail [privacy@t-mobile.com](mailto:privacy@t-mobile.com) [11], or write to:
  
  T-Mobile USA, Inc.  
  Attn: Chief Privacy Officer  
  12920 SE 38th Street  
  Bellevue, WA 98006

- **AT&T**: Go to [www.att.com/gen/privacy-policy?eid=2506](http://www.att.com/gen/privacy-policy?eid=2506) [12] to read the privacy policy, e-mail [privacypolicy@ATT.com](mailto:privacypolicy@ATT.com) [13], or write to:
  
  AT&T Privacy Policy  
  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 [14].

- **Sprint**: Go to [www.sprint.com/legal/privacy.html](http://www.sprint.com/legal/privacy.html) [15] to read the privacy policy, e-mail [officeofprivacy@sprint.com](mailto:officeofprivacy@sprint.com) [16], or write to:
  
  Office of Privacy-Legal Department, Sprint Nextel  
  P.O. Box 4600
b. What Other Data Should You Be Aware of on Your Smartphone?

In addition to the data collected by your smartphone service provider, you should also be aware of the possible privacy issues surrounding the collection or disclosures of:

- Any photos or video you take on your phone;
- Details about the text messages and e-mails you send and receive, including the content;
- Who is calling you, who you are calling, and details about the phone call such as when it was placed and how long it lasted;
- The contacts you have stored in your phone;
- Passwords;
- Financial data;
- What you store in your phone's calendar;
- Your location, age, and gender.

3. Who would want to snoop on you using your smartphone?

Criminals, advertisers, and—in some situations—the government would love to get their hands on the data stored in your smartphone:

a. Criminals

A cybercriminal may want to: steal your money, collect personal data to commit identity theft, harass or stalk you. 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?

Consumer Privacy Tips:

- Password protect your phone. As always, make sure you use a strong password. For tips on creating an effective password see PRC’s “10 Rules for Creating a Hacker-Resistant Password”[17]. You can usually find the feature allowing you to set a password in the phone settings.
- Do not allow your smartphone to automatically remember login passwords for access to email, VPN, and other accounts.
- Use your phone’s security lockout feature. Set the phone to automatically lock after a certain amount of time not in use.
- Also install security software that allows you to remotely lock your phone and wipe the data. Never leave your phone unattended.

ii. Malware

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, 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 as well.

Unfortunately, mobile malware attacks are on the rise in part because individuals are less likely to guard their smartphones in the way they do their computers. Also, attacking a smartphone may provide criminals with quick rewards because the increasing popularity of mobile payment options allows criminals to directly profit off of their attack. Criminals can also profit by directly charging to an individual’s phone bill.

iii. Geotags

Depending on the settings, your smartphone may be using its built-in GPS capability to embed your exact location into the file of photos you take using the smartphone’s camera. 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.

Consumer Privacy Tip: Disable photo geotagging on your phone. See instructions at I Can Stalk U: How Do I Disable This?[18]

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. Therefore, they are very interested in what your smartphone has to “say” about you as a consumer.

Currently, applications (or apps) are widely used by advertisers to capture your smartphone data. The 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. Apps

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 which is shared with advertising networks. The advertising 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.

In December 2010, the Wall Street Journal investigated 101 apps[19] to see what data the apps were sharing with advertisers. It found that 56 apps shared the phone’s unique ID number, 47 transmitted the phone’s location and 5 shared the user’s age and gender and other personal details (like phone number or contacts list).

The Federal Trade Commission has published a guide “Marketing Your Mobile App: Get it Right from the Start”[20] to help mobile application developers observe truth-in-advertising and basic privacy principles when marketing new apps.

One concern surrounding applications and their ability to share and sell user data is that many apps do not have privacy policies. Even when an app has a privacy policy, the small size of a smartphone screen combined with complex and lengthy policies may make the policies both difficult to read and to understand.

Consumer Privacy Tips:

- Research apps before you download them. Look at how many people have downloaded the app, read what they have said about it, determine who created it, and if you are skeptical do some further research. Look up the app’s privacy ratings on Clueful.[21]
- Look for a privacy policy and terms of service. If the app download screen doesn’t show it, usually the app’s webpage will, but you might have to do a little hunting. See our Fact Sheet 35, section 8: Reading a Privacy Policy.[22]
- Ask yourself, “Is this app requesting access to only the data it needs to function?” If the answer is no, don’t download it. 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 have an install screen, but you can see which apps want to access your location by going to Settings > General > Location Services. If you are not using Android or iOS, research your particular operating system to educate yourself on this practice.
- Contact your lawmakers. Also, look for opportunities to comment to the Federal Trade Commission if you have opinions or ideas about how to ensure that consumers are given adequate notice and choice with respect to mobile data practices.
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 a consumer 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 behavioral 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 [23].

To learn more about behavioral marketing, read this section of PRC's Fact Sheet 18: Online Privacy: Using the Internet Safely [24].

c. The Government

The ability to collect data on where a person has gone and what they have been doing is valuable information for law enforcement officers. For example, 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. Thus, the data provided by your smartphone may be used against you in a court of law.

The Fourth Amendment to the Constitution protects you from unreasonable searches and seizures by law enforcement. However, depending on your jurisdiction, there are different requirements for when and how law enforcement may access cell phone data without a warrant. For example, whether police may search the contents of a cell phone if you are arrested or pulled over may vary depending on what state or federal court circuit you are located in.

Law enforcement has also been known to tap into the locations of smartphones, ask wireless providers to turn over days' worth of location data, and implant tracking devices. Also, law enforcement can request all the data your smartphone provider has collected about you. 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.

NOTE: For more information, please see the ACLU's site on surveillance [25].

4. How Are Smartphones Attacked?

a. Criminals Can Physically Gain Access to Your Smartphone

A person who gains access to your smartphone can physically install surveillance spyware. An online search for "smartphone spy" pulls up software that promises "it doesn't matter if the user tries to delete their tracks by deleting their data. This flexible spy software records the activities instantly after they happen and stores them to a small hidden file on the phone. The file is then uploaded to your web-based account."

Even scarier, certain spyware can "turn on" your phone's microphone and camera, using it to listen and see what's going on around you. Spyware can also track and record your location. Unfortunately, it can be very difficult to detect spyware on your own.

Consumer Privacy Tips: These tips are also listed above.

- Password protect your phone. As always, make sure you use a strong password. For tips on creating a hacker resistant password see PRC's "10 Rules for Creating a Hacker-Resistant Password" [17]. You can usually find the feature allowing you set a password in the phone settings.
- Do not allow your smartphone to automatically remember login passwords for access to email, VPN, and other accounts.
- Use your phone's security lockout feature. Set the phone to automatically lock after a certain amount of time not in use.
- Also install security software that allows you to remotely lock your phone and wipe the data. Never leave your phone unattended.

b. 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 has VPN or SSL protection. This data could be what you are typing (worst-case scenario: 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. Turn off your Bluetooth function when you are not using it.

Consumer Privacy Tips:

- Use public Wi-Fi networks cautiously. Do not conduct activities that use sensitive information such as mobile banking.
- 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 [26] to learn more.

c. By Trickying You or Exploiting Your Trust

Often, cybercriminals work by exploiting consumer trust and convincing them that their links, URLs, applications or files are safe. However, they may also infiltrate legitimate software. Therefore, we recommend that you install your choice of mobile security software.

Consumer Privacy Tips:

- When clicking on links, downloading files, and downloading apps, make sure you are aware of and trust the source.
- Look into installing security software on your smartphone.

5. Mobile Security Software

Many individuals take great care to protect their computers with security software, but forget to address the security of their smartphones. Don't neglect your smartphone's security. Products include Lookout Mobile Security, AVG, McAfee, and Norton. Some products are even free. (No endorsements implied.)

Depending on the software, you may be able to protect against malware, back up your smartphone data, store data elsewhere, track your phone if it is lost or stolen, protect against certain viruses, lock your phone remotely, and wipe your data remotely.

However, as with anything else you download on your smartphone, be sure to research mobile security companies and software before you download. Don’t allow someone to exploit your trust just because they say they are providing you with a security service. Also, research privacy policies—the company may be giving free security software so that it can get your personal data.

6. Privacy Issue to Monitor: Applications

The popularity and increasing availability and quantity of downloadable apps is a top privacy issue. People are increasingly spending more time using mobile applications than they are browsing the mobile web. There are hundreds of thousands of apps available for your smartphone, and anyone can create an app. The app marketplace is filled with numerous free or low-priced choices. Apps can collect all sorts of data and transmit it to your smartphone or third-party advertisers. It can then be shared or sold. Apps may also be infected with malware.

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.


A July 2012 study by the mobile security company Lookout found that ads from advertising networks running on some apps may change smartphone settings and take contact information without your
permission. The study tested 384,000 apps and found that 19,200 of those apps used malicious ad networks.

When you install an app, you allow it to access certain data on your phone. One of the most common complaints is that many apps track your location. There are location-based services like Yelp and Foursquare that need your location in order to function properly (read ACLU of Northern California's Location-Based Services: Time for a Privacy Check-in [PDF] [39]). However, there are also apps that do not need your location to function and yet still track it.

During the 2012 presidential campaign, apps created by both major candidates to promote their election campaigns gathered (or sought permission to gather) large amounts of personal information including GPS location data. http://www.networkworld.com/news/2012/082112-obama-and-romney-election-apps-201208.html?pg1=1 [39].

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.

However, many mobile apps do not have privacy policies [31], and when they do, they are often dense with legalese, lengthy, and difficult to read on smartphone screens. The Mobile Marketing Association [32] offers resources for mobile app developers interested in creating a privacy policy. Despite their efforts, mobile app privacy is far from standardized and is a developing area in both the policy and legal realms.

To learn more about the direction and policy strategy the mobile industry is taking, you may want to visit CTIA-The Wireless Association’s best practices on location based services, [33] CTIA is an industry group representing the wireless communications industry.

Consumer Privacy Tips:

- As mentioned above, we urge you to research apps before you download them and to turn off location-tracking for the apps that don’t need it.
- Certain smartphones may ask you for specific permissions when you install an app. Read these, think about what the app is asking for permission to access and what it does for you, and make an educated decision. 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.
- Consider writing to the companies involved (such as Apple and Google) and request stronger safeguards for apps to protect your data from being shared with third-parties without your prior consent.

7. Do We as Consumers Have Protection?

Unfortunately, laws have not kept pace with changing technology. The first iPhone was released in 2007, and since then there has been an explosion of smartphone 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. We urge you to become familiar with the work of the American Civil Liberties Union [34], Electronic Frontier Foundation [35], and the Electronic Privacy Information Center [36] for more information.

b. Existing Federal Law

i. The Electronic Communications Privacy Act (ECPA)

Enacted in 1986, 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 [37]. 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 [38] (18 U.S.C. § 1030) was enacted to prevent unauthorized access to computers. 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. In fact, as of April 2011, a federal grand jury was investigating app makers to see if they have breached this Act by transmitting smartphone data to third parties. To learn more, read Wall Street Journal: Mobile-App Makers Face U.S. Privacy Investigation [39].

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

The 1998 COPPA (15 U.S.C. §§ 6501-08) 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.

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 [40]. If you suspect that a site or application is not complying with COPPA you can file a complaint with the FTC [41].

To learn more about COPPA visit:

Center for Digital Democracy [42], CDD is a non-governmental organization with resources on digital marketing, digital health issues, digital privacy issues, and youth digital marketing.


c. The Federal Trade Commission

The FTC [44] recognizes smartphone privacy issues, including those involving mobile apps. In February 2013, the FTC issued Mobile Privacy Disclosures: Building Trust Through Transparency: A Federal Trade Commission Staff Report [45]. The report makes recommendations for players in the mobile marketplace: mobile platforms (operating system providers, such as Amazon, Apple, BlackBerry, Google, and Microsoft), application (app) developers, advertising networks and analytics companies, and app developer trade associations. Most of the recommendations involve making sure that consumers get timely, easy-to-understand disclosures about what data they collect and how the data is used.

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. Whether or not a company is required to have a privacy policy depends on varying state laws. However, if a company does have a privacy policy and you find it in violation of its privacy policy, you should file a complaint with the FTC. This is why it is so important to read privacy policies carefully.

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

d. State and Federal Legislation Applying to Smartphone Use

Smartphone privacy, in particular geolocation privacy, has been a hot topic in Congress. You can research bills being considered by Congress by visiting the official website of the Library of Congress, Thomas [46], and using its search feature for the word “geolocation.”

To learn if your state has any laws on the books on geolocation privacy, or if your state legislature is considering a bill on that topic, visit the website of the National Conference of State Legislatures [47] and use its search feature.

Consumer Privacy Tips:

- 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.
8. Summary of Consumer Privacy Tips

1. Never leave your smartphone unattended.

2. Use public Wi-Fi networks cautiously and turn Bluetooth off when not in use. Read Lifehacker: How to Stay Safe on Public Wi-Fi Networks [38] to learn more.

3. Disable photo geotagging on your phone. See instructions at I Can Stalk U: How Do I Disable This? [18]

4. Research apps before you download them:
   a. When browsing an app store, look at how many people have downloaded the app you are interested in and what rankings they have given it.
   b. Look for a privacy policy and terms of service. If the app download screen doesn't show it, usually the app's webpage will, but you might have to do a little hunting. See our Fact Sheet 35, section 8: Reading a Privacy Policy [29].
   c. Ask yourself, "Is this app requesting access to only the data it needs to function?" If the answer is no, don't download it.

5. Consider writing to the companies involved (such as Apple and Google) and request stronger safeguards for apps to protect your data from being shared with third parties without your prior consent.

6. Password protect your phone. You can usually find this feature in the phone “Settings.” Never leave your phone unattended. Do not have your smartphone remember login passwords for access to email, VPN, and other accounts.

7. When disposing of, recycling, or donating your smartphone, be sure to remove the SIM card and wipe or reset the phone first. Thieves may prey upon phone recycling kiosks. For a guide to wiping data on your smartphone, see this Consumer Reports (updated February 2015) article [49]. Be aware that some Android phones cannot be wiped clean [50].

8. Write to your Congressional Representatives. Tell them that we need to update existing privacy law in order to keep pace with changing technology.

9. The FTC does not resolve individual complaints, but if you believe that a particular company is engaging in wrongdoing (for example if it has violated its privacy policy) you can submit a complaint [41].

10. Try the Federal Communications Commission's interactive Smartphone Security Checker at http://www.fcc.gov/smartphone-security [51]. This online tool creates a 10-step action plan to help consumers protect their mobile devices from smartphone-related cybersecurity threats.

9. Resources

a. Government and Non-Governmental Organizations

   - ACLU:
     2. ACLU of Northern California’s Location-Based Services: Time for a Privacy Check-in: http://www.dotrights.org/LBS [52]


   - Privacy Rights Clearinghouse: Consumer Guide, Mobile Health and Fitness Apps: What are the Privacy Risks? [54]


   - New Media Rights Videos: Cell Phone Tracking: http://www.newmediarights.org/how_toconsumerremoves/how_identify_and_remove_cell_phone_tracking_software [56]

   - New Media Rights Videos: Mobile Privacy Disclosures: Building Trust Through Transparency: A Federal Trade Commission Staff Report [57]


   - California Attorney General, Privacy on the Go: Recommendations for the Mobile Ecosystem [69]


   - Federal Trade Commission, Understanding Mobile Apps [61]

b. Media & Industry Resources


     Phone: (866) 211-0874
     Email: privacyoffice@verizon.com [7]

     Phone: (877) 937-8997
     Email: privacy@tmobile.com [11]
     Mail: T-Mobile USA, Inc. Attn: Chief Privacy Officer 12920 SE 38th Street Bellevue, WA 98006

     Email: privacypolicy@ATT.com [13]
     Mail: AT&T Privacy Policy 208 S. Akard Room 1825 Dallas, TX 75202
Where to Complain

- Federal Communications Commission (FCC)
  Online: http://esupport.fcc.gov/complaints.htm
  Phone: (888) 225-5322
  TTY: (888) 335-3322
  Fax: (666) 418-0232
  E-mail: fccinfo@fcc.gov
  Mail: Federal Communications Commission
        445 12th Street SW
        Washington, DC 20554

- Federal Trade Commission (FTC)
  Online: Use our secure complaint form.
  Phone: (877) 382-4357
  TTY: (866) 653-4261
  Mail: 600 Pennsylvania Avenue, NW
        Washington, DC 20580

Source URL (modified on June 3, 2016): https://www.privacyrights.org/consumer-guides/privacy-age-smartphone