



## Mobile Phones: Balancing Privacy and the Law

Very few innovations have had such an immediate and indelible impact on human behavior as the mobile phone. But what's even more fascinating is its blistering-fast evolution from [brick-shaped audio handset](#) to pocket-sized, do-it-all communications computer.

Like many technological breakthroughs however, the mobile phone has led to several legal entanglements. Specifically, for litigation attorneys, the valuable location information, call logs and text messages contained in the phone (or retained with the service provider) can potentially be accessed by authorities looking for information regarding a specific case. This opens a proverbial [Pandora's Box](#) of privacy concerns.

### WHAT KIND OF DATA CAN A PHONE CONTAIN?

A quick glance at all the icons on your phone's home screen will tell you that gizmo packs way more tech than a walkie-talkie. So, without diving into a deep technical discussion, let's explain in very basic terms how a mobile phone works first before addressing some of the privacy issues at play.

To connect to the data network, a phone relies on nearby towers to relay its signal. So, when you're sitting in your office, riding in a car or eating at a restaurant, your phone is always reaching out to the nearest nodes to connect to the network—which means you're essentially being tracked every moment that it's powered on.

Though that capability can be a valuable asset in an emergency, it also means that your phone data can now indicate your general whereabouts to anyone who has access to that information. You'll read more about the court decision that made that possible further in this article.

A smartphone can also store call records, contacts, text messages, emails and more—and often that information can be accessed by the phone's service provider without the need to have possession of the physical phone.

### RECORDED PHONE CALLS AND THE COURTS

For the “phone” part of a smartphone, the laws can be pretty clear. For a bit of history, there are some court decisions to look at, perhaps starting with 1956's *Rathbun v. United States* (*Rathbun v. United States*, 236 F.2d 514). If you're a Lexis Advance® user, you can get a [deep look into the case here](#), but it essentially involved a phone conversation between two parties, with police (invited by the first party) listening-in unbeknownst to the other party.

Phone call recordings can be used in litigation, and most states currently only require one party to consent to the recording—though there are several (10+) two-party consent states..

---

## CAN THE POLICE SEARCH YOUR PHONE?

This is a topic that's been in the news a lot recently, and it's been addressed by the United States Supreme Court. It's important to realize too that when talking about data, it can mean both the information stored on the phone itself and the information possessed by the phone company.

Take a look at 2018's *Carpenter v. United States* (*Carpenter v. United States* 138 S. Ct. 2206/138 S. Ct. 2206), the details of the case can be found [here at Ravel™ Law](#). The decision basically stipulated that law enforcement officers must obtain a search warrant before they can get your phone data. (It's important to note that this law may not apply in emergency situations whether there is considerable risk of loss of life or damage to property.)

And that's a big deal, because, as alluded to above, your phone contains a lot more data than just call records and contacts.

## A LEGAL GREY AREA

You may recall a 2016 dispute between Apple® and the FBI concerning Apple's role in unlocking a private citizen's iPhone®. The citizen in question was one of the shooters in the terrorist attack in San Bernardino, California. The FBI had possession of the phone and wanted Apple to give them access to the information it held. Apple challenged the order—however, days before the hearing, the FBI was able to access the iPhone without Apple's assistance. The FBI withdrew its request and the challenge was rendered moot.

A more [recent story found on NBCNews.com](#) concerns an individual who, during a police stop, was ordered to provide officers his password to unlock his phone. The gentleman refused on privacy grounds. While this particular case is nuanced, a key takeaway here is that, while a court-ordered warrant may permit access to phone data, it's not clear whether law enforcement agencies can order citizens to provide access to their phones on the spot. Privacy advocates point to the Fifth Amendment in a lot of these situations.

## A BALANCING ACT

As Uncle Ben famously told a young Peter Parker, "[With great power comes great responsibility.](#)" Perhaps it's fair to adapt that logic to mobile phones. What level of privacy are we willing to give up for convenience and safety? Or, perhaps more accurately, what level of trust are we comfortable giving to the law enforcement and tech sectors?

Legislation is notorious for lagging behind technology. And, given the rapid pace of smart phone development, it's no surprise that laws and precedent simply don't exist (yet) to address all of the facets of data privacy. Expect related legislation to play catchup for the foreseeable future.

---

## About LexisNexis® Legal & Professional

[LexisNexis Legal & Professional](#) is a leading global provider of content and technology solutions that enable professionals in legal, corporate, tax, government, academic and non-profit organizations to make informed decisions and achieve better business outcomes. As a digital pioneer, the company was the first to bring legal and business information online with its Lexis® and Nexis® services. Today, LexisNexis Legal & Professional harnesses leading-edge technology and world-class content to help professionals work in faster, easier and more effective ways. Through close collaboration with its customers, the company ensures organizations can leverage its solutions to reduce risk, improve productivity, increase profitability and grow their business. LexisNexis Legal & Professional, which serves customers in more than 175 countries with 10,000 employees worldwide, is part of RELX, a world-leading provider of information and analytics for professional and business customers across industries.

