Online activity is always growing, especially as the Internet of Things develops (IoT). Requests for data are continually hammered into our ears. Identity theft instances, phishing scams, and scam websites are all always on the rise. Being extremely watchful regarding the security of your information is crucial now more than ever. Furthermore, a key component of your right to privacy is understanding precisely who has access to and how they utilise your personal information.

You want to be totally certain of where and how your information is going, whether you're giving out your e - mail address or making online purchases. As a result, becoming familiar with the fundamentals of fair information practises will aid you in making the appropriate choices as you move between offline and online settings. You'll also be able to report those organisations that aren't adhering to best practises, which will assist to make the environment safer for all users thanks to your increased knowledge.

Notice refers to the requirement that the information provider be informed of the precise recipients and purposes of the information. This, also known as transparency, is crucial in order to give the customer the information they need to decide whether or not to share their information and what information they want to share. As applicable, an entity should cover a few of the following:

* Who is collecting the information
* What it will be used for
* Who could potentially receive the data
* What information will be collected and how
* Whether providing the data is optional
* How the collector will ensure the confidentiality, quality, and integrity of the information
* If and when the information will be disposed of

These steps are frequently bypassed, especially if the user already has some level of trust in the institution that is collecting the data. However, in some circumstances you can be much more likely to search phrases and policies for pertinent information. Consider the scenario where you specifically use a company's services for data protection. You should fully understand how each company plans to manage your data if you're looking for a VPN service or browser privacy extension.

**Choices should be offered, and consent required**

In basic terms, this principle gives consumers the right to decide how their information is used. This refers more to secondary use, as the primary use will typically be evident, for example, to sign up for a service, complete a purchase, or access a piece of content. Beyond the primary reason, entities may want to record and use your data for other purposes, such as to add you to their own or other companies' email lists. Any data use beyond the obvious should be clearly laid out. Plus, the consumer should have the option of whether they want to give their consent for their information to be used in the manner specified.

A common example is the option to receive promotional information from whichever entity you are handing your information to, as is the case with the [California Lottery signup form](https://www.calottery.com/register):

**3. Consumers should be able to access and alter data**