Increasing Number of Devices - The number of interconnected sensors and smart devices is growing exponentially, increasing the opportunity for attacks.

One design concern around privacy is the question as to who can access private data. The creator of a website or an app should clearly make the private data available only to specific people they deem necessary and appropriate.

Some issues with securing IoT devices are:

* **Increasing number of devices** – The number of interconnected sensors and smart devices is growing exponentially, increasing the opportunity for attacks.
* **Non-Traditional Location of Devices** – Some connected IoT devices can interact with the physical world. They are now located in appliances, in automobiles, on or in our bodies, and in our homes. Sensors may gather data from the refrigerator or the heating system. They could also be in city lampposts or attached to tree trunks. These non-traditional locations make physical security difficult or impossible to achieve. Attackers may have direct physical access to IoT devices. Given the highly interconnected nature of IoT devices, this can create a situation where a weak link in a small sensor or actuator could jeopardize security locally or globally.
* **Lack of upgradeability** – IoT sensor-enabled devices may be in remote and/or inaccessible locations where human intervention or configuration is almost impossible. These devices may also contain basic technology designed for one simple task. The devices are often designed to be in service many years longer than is typical for conventional high-tech equipment. It is possible that these devices could outlive the company that created them. This creates the possibility of having installed devices with no means of long-term support.

Some methods that can be used to overcome these privacy and security issues are:

* **Transparency** – People should know what types of personal data are being collected, why the data is being collected, and where it is to be stored.
* **Data collection and Use** – Smart devices should only store personal data that is adequate and relevant in relation to the purpose for which they are collected. Data that hides the identity of the person should be used wherever possible.
* **Data access** – Before new systems are deployed, designers should determine who is able to access personal data collected by smart objects and under which conditions. If appropriate and clear procedures are established and promoted, people affected by the devices can make their own judgement about using the system.