|  | **iBeacon** | **NFC** | **RFID** | **GPS** |
| --- | --- | --- | --- | --- |
| **Accessibility** | With smartphones primarily acting as receivers, beacons form a highly accessible indoor location technology. | Deploying a NFC system requires a number of components such as tags, readers and reader control and application software to be in place. Therefore, businesses that plan to go ahead with NFC need to plan and invest upfront in new infrastructure. | Deploying an RFID system requires a number of different components, including basic hardware such as tags, readers, reader control and an application software. Furthermore, while most location solutions come with an inherent compatibility with mobile, RFID does not. | GPS is a highly accessible technology. |
| **Range** | Beacons typically have a wireless range of 1m to 70 m. | NFC works at an optimal range of 10cm or less. | RFID uses three main frequencies:  125 – 134 KHz­ Low Frequency with range up to 1 -10 cm,  13.56 MHz High Frequency and NFC with range 1 cm – 1 m,  865 – 960 MHz Ultra High Frequency with range 5 – 6 m (but even more with the right conditions). | In this case, the range is unlimited. |
| **Accuracy** | Beacons being radio transmitters are not very accurate as they stand the chance of interference, as radio signals can be absorbed by different media, such as water, air, human bodies or even metallic surfaces. | NFC is an averagely accurate indoor location technology for near range alone. | Its accuracy varies based on a number of factors, primarily frequency, tag antennas, readers and reader antennas.  Ultra High Frequency has bad accuracy. | A number of factors such as atmospheric effects, sky blockage etc, play a critical role in the accuracy of GPS. Generally, high-quality GPS receivers provide a horizontal accuracy of more than 3.5 m. Higher accuracy in the range of centimeters is attainable by using GPS in combination with augmentation systems. It wasn’t designed to do indoor localization. |
| **Security** | Beacon Hacking, a common threat to beacon security occurs when beacons with weak security measures are discovered by hackers who then change their UUIDs, Majors and Minors to leverage the beacon network without prior permission. Most beacon manufacturers have now put some measures in place to prevent this from happening. | NFC supports encryption and since it requires close proximity between devices for proper functioning, the odds of a hacker intercepting the signal is minimal. | Since RFID systems are closely tied to standard IP network security solutions, any IP communication between RFID readers and the network is very secure. However, the only real security threat lies in the RF communication that happens between the tags and readers. Few common forms of data security threats are rogue/clone tags, unauthorized riders, and side-channel attacks. | GPS by itself is not invasive and the privacy and security risk associated with GPS mainly comes from the receivers (devices) and communication mechanism inherent in the manufacturer's servers. Most manufacturers these days employ various authentication and storage techniques to secure a GPS receiver. |
| **Ease of use** | Consumers respond to notifications that are triggered on their smartphone when they are within the range of a beacon. | Consumers use a NFC tag to control timing and engagement. | Consumers need to carry around a RFID tag. | Consumers have to switch on the GPS on their smartphones. |
| **Energy Efficiency** | Majority of beacons are battery powered and last for up to one year before they need to be replaced. You can even find, USB powered and electromagnetic wave powered beacons in the market these days. | NFC does not need power to function. Each NFC tag creates its own power when it is in the presence of an NFC-enabled smartphone. | RFID energy consumption depends for the most part on the frequency used: the higher the frequency, the more power will be consumed. | Constantly searching for satellites can result in a huge battery drain. Thus, when it comes to an "always-on" use case, GPS is a poor solution to go ahead with. |
| **Privacy** | Beacons can be more intrusive as irrespective of who deployed the beacons, a mobile app can be configured to monitor consumer movements as they move along. | NFC is less intrusive as the movements of a consumer can only be monitored based on the NFC tag that they have engaged with. No third party, other than the one who has supplied the tag contents can monitor engagement. | A major concern over the increase in use of RFID tags is the personal security associated with the illicit tracking of RFID tags. Some approaches can be implemented to strengthen the system. | Privacy risk associated with GPS mainly comes from the receivers (devices) and communication mechanism inherent in the manufacturer's servers. |
| **Inherent capability of smartphones** | iBeacon only requires devices to have Bluetooth LE installed in them, which many smartphones already have. | Neither Apple products prior to iPhone 6 nor other popular smartphones come with an inherent NFC chip. | To date, all major smartphone manufacturers are of the opinion that customer value does not justify the cost or complexity of building it into a mobile device. That said, it is still possible to download software or add attachments to turn a mobile device into a reader. | It is an inherent capability of all smartphones. |