beacon

INTEGRATED PRIVACY PROTECTION SYSTEM

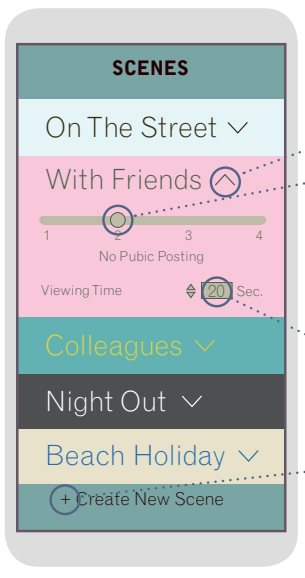
There are more and more cameras pointed at us on the street, in our stations and malls, not to mention the smartphone cameras we so happily keep in our pockets. And, together with the surprising accuracy of the advanced facial recognition technologies, it is said that we will soon be forced into giving up the anonymity outside of our houses.

Beacon is a concept of an integrated privacy protection system. It effectively brings back to us the right to our own facial images by limiting, and sometimes disabling, the cameras around and the ability to digitally share the pictures taken.

1. Determining Privacy Settings

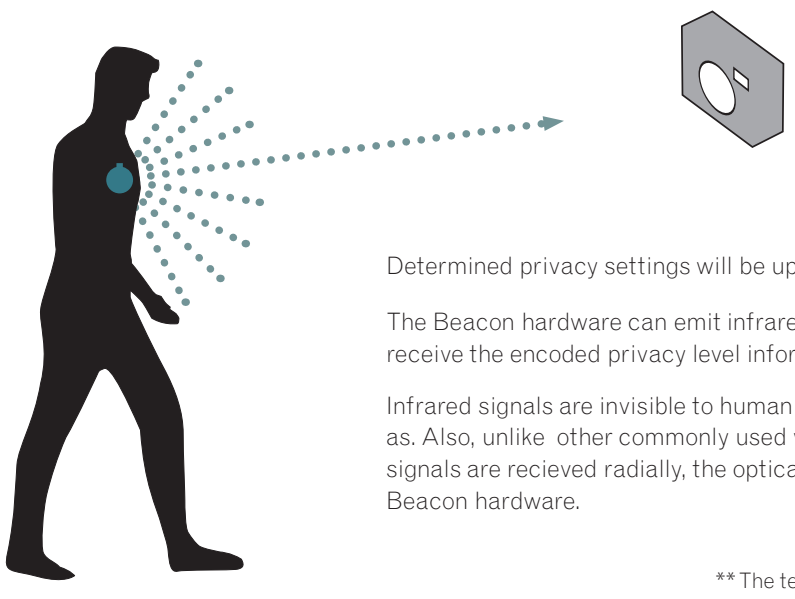
On Beacon mobile app, users determine the levels to which they want their pictures to be shared.

Depending on the occasions we are in, we naturally have different levels of reasonable expectation of privacy. Those occasions are called Scenes on the app, and the privacy levels can be fine-tuned separately in each of them. Also, new Scenes can be freely added by the users' preferences.



- Tap on the arrow to open and close each Scene
- Privacy levels can be managed by sliding the button up and down
  1. No Sharing Limits : Pictures are free to be shared with anybody on any platforms
  2. No Public Posting : Pictured faces cannot be posted online to public platforms
  3. No Forwarding : Pictured faces sent cannot be forwarded further than the first recipients
  4. No Photos : Faces pictured are made invisible by blurring
- Viewing Time, after which pictured faces become blurred, can be adjusted
- To create new Scenes, tap on the +

2. Wearable Hardware



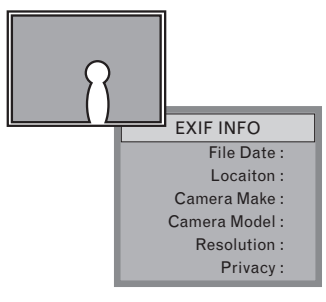
Determined privacy settings will be uploaded to the Beacon hardware.

The Beacon hardware can emit infrared signals toward cameras pointed at it, for them to receive the encoded privacy level information determined by the user.

Infrared signals are invisible to human eyes, but still can be read by compatible digital cameras. Also, unlike other commonly used wireless communication methods such as WiFi, whose signals are recieved radially, the optical signals will affect only the cameras pointed at the Beacon hardware.

** The technology to control cameras through infrared communication is based on a patent granted to Apple in 2016. Details **here.**

3. Embedding Metadata Into Pictures



The cameras receivng Beacon's signal will embed metadata into all the pictures it takes.

The picture files come out tagged with the user's desired privay level on them, together with other common types of metadata to accompany pictures, such as date, geotag, camera model, resolution, and so forth.

4. Sharing Controlled

The picture files can be handled and shared only as they are intended by the wearer of the Beacon hardware.

The original privacy settings on the mobile app are passed down all the way through to the final viewers, and the attemps to share with unintended devices or platforms will be blocked.