



BEST PRACTICES:
**BEACON LOCATION SECURITY
AND ENCRYPTION**

A small white icon of a padlock is positioned at the end of the title text.

JAMES BUCHHEIM, CEO

BEACONS OVERVIEW

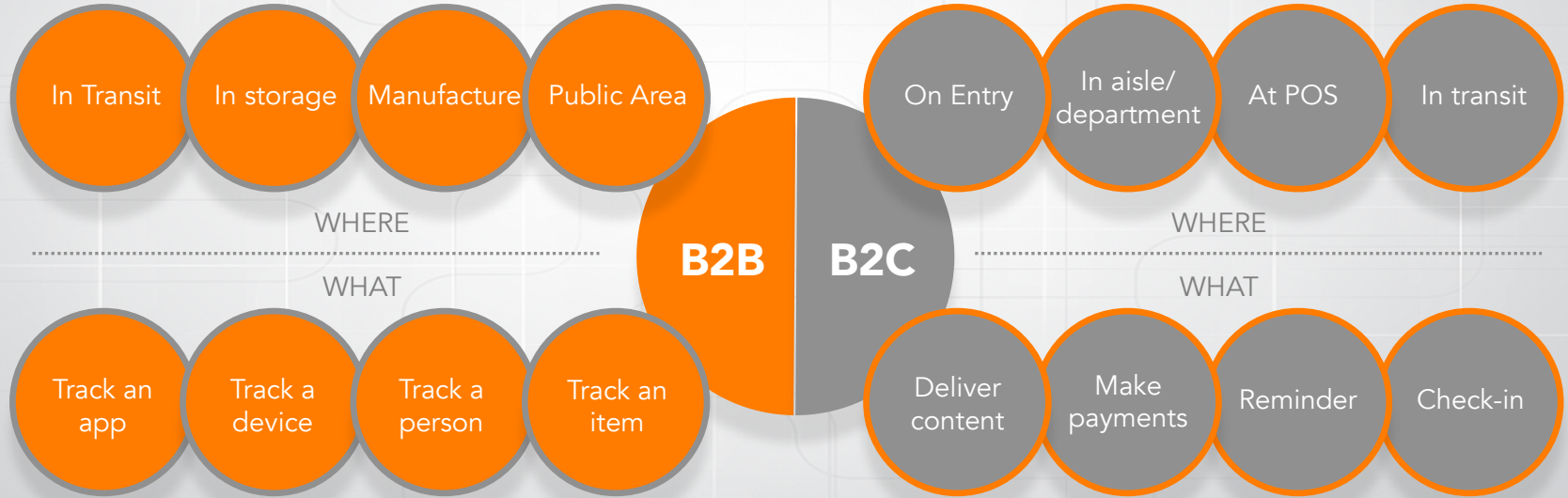
- *Beacons interact with standard mobile devices and applications*
- *Simple, inexpensive, small and long-life battery-powered*
- *Key advantage: Contextual engagement at right place, right time*

BEACONS TRENDS

A small white icon of a beacon or tag is positioned at the end of the title 'BEACONS TRENDS'.

- *Apple iBeacon Hype: iBeacon is just A Protocol*
- *Google standardized BLE*
- *IoT with unlimited contextual apps and discovery services*
- *Beacon Cloud-based ecosystem a MUST for management*
- *Privacy and Security Challenges – Extreme care and security to ensure beacons respect Privacy (based on a GSMA study)*

THE OPPORTUNITY



VERTICAL OPPORTUNITY



B2C SECTORS



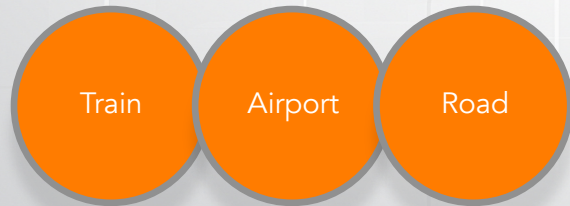
Healthcare



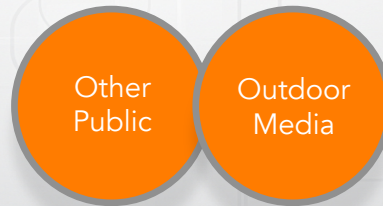
Retail



Entertainment



Transport



Advertising



Hospitality

PROTECTION

Deployer (Enterprise)



- *When? Care should be taken when deploying beacons to ensure their infrastructure cannot be used by unauthorized third parties*
- *Where? In any third party apps or customer identifiable data collection*
- *How?*
 - *Use a non-deployer unique UUID*
 - *Ensure Major And Minor schema is not decodable by 3rd parties (random)*
 - *Change major and minor frequently (example: once per minute)*
 - *Deploy and configure with a secure, private password*

PROTECTION

User (Customer)

A small white location pin icon is positioned at the end of the 'User (Customer)' text.

Four Best Practice findings identified:

- 1. Always offer customer value in return for knowing their location*
- 2. Ensure customers fully understand how their location data used/recorded*
- 3. Take steps to protect live or historical data in mobile app or other platform*
- 4. Do not share user location data with 3rd parties without permission(s)*

PROTECTION SCHEMES



UUID

- Used in beacon settings to identify the owner/deployer

MAJOR/MINOR

- Major identifies location
- Minor Identifies micro-location within a location

Single

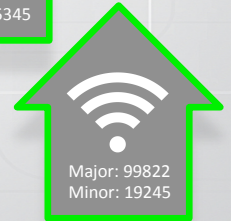
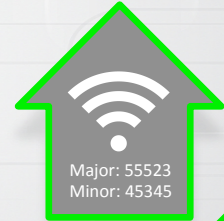
UUID: F8AD3E82-0D91-4D9B-B5C7-732474426



UUID: B9407F30-66...9-25556B57FE6D



UUID: A7408V30-6...8U1-25556B57A96R



Retailer A

Retailer B

ENCRYPTION

- *Data encryption protection can be implemented on beacon or cloud services*
- *Apps that carry trigger value transactions should utilize encrypted beacons*
- *Sellers and deployers of beacons should provide guidance on why and how to utilize beacon technology in a responsible and secure manner and consider the benefits of adding encryption*

CLOUD PLATFORM

New Secure Way



Three Basic Security/Encryption Models:

- 1. STANDARD:** *App holds all beacon estate data locally*
- 2. CLOUD:** *App queries a cloud-based platform with UUID, Major and Minor for location data returned*
- 3. CLOUD SECURE:** *Beacon data is fully encrypted and only decrypted by cloud platform, which returns to the app detailed location data*



NEXT STEP

Beacons Security/Privacy



- *Meet StickNFind in exhibit area to learn more on managing cloud security with our new BluZone beacon cloud-based beacon control dashboard*
- *Email @ jimmy@sticknfind.com*