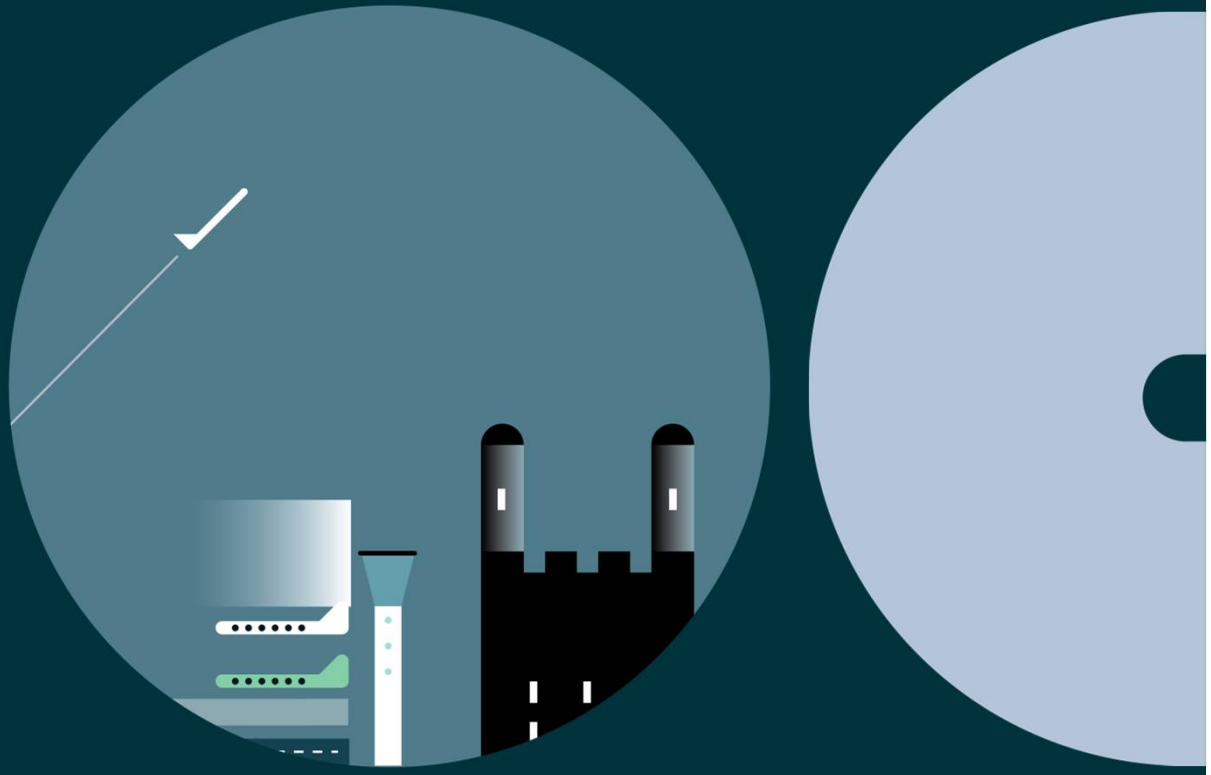
Mobile App and Beacon Privacy



Stephen Groom

30 September 2014

Mobile apps/beacons: examples of potential personal data involved

- Location data
- Contacts
- Unique device and customer identifiers (e.g. IEI,IMSI, UDID and phone number)
- Data subject identity
- Store activity data

- Credit card and payments data
- Phone call logs, SMS or instant messages
- Browsing history
- Email
- ISS authentication credentials

The regulators are circling…

Sept '14 – Global Privacy Enforcement Network 26 country app sweep

Key findings:

1. 59% of apps offered little info, prior to download, on how data was collected or used

2. 43% of apps failed to tailor privacy notices to the small screen

3. Only 15% of apps gave a clear explanation of how they would collect, use and disclose personal information

Be an instant in-store beacon/app ("ISBA") privacy law expert! #1

So you have an idea for an ISBA app. When is the best time to think about privacy law compliance?

1. When determining core functionality ***Correct answer***

2. Before publishing your API

3. Five working days before launch

Be an instant ISBA privacy law expert! #2

iBeacons enable an app-equipped mobile to use store location data to deliver real-time personalised marketing messages. Do you:

1. rely on Bluetooth being turned on as an indication of consent to use of location data?

2. ensure the mobile user/subscriber ("U/S") gives informed consent on signing up for the app? ***Correct answer***

3. assume it's all covered in the U/S's contract with the telecoms service provider ?

Be an ISBA privacy law expert! #3

As a retailer negotiating an agreement for a developer's supply of an ISBA solution, do you:

1. Leave it to your IT/legal teams to do a privacy impact assessment and advise on compliance later?

2. Say in the agreement who takes responsibility for which aspects of data privacy, data security and electronic comms law compliance and who is data controller? ***Correct answer***

3. Expressly agree that both parties will comply with the Data Protection Act 1998 and related legislation?

Be an instant ISBA privacy law expert! #4

The ISBA will exchange U/S data with the retailer's CRM database and thereby enable ever more targeted engagement with the U/S. As the developer do you:

1. Assume the U/S already gave consent to his/her CRM database data being enriched by other data?

2. Cover it off in the app privacy notice the U/S sees after installing the app?

3. Check that previous retailer privacy notices disclosed possible appending to the U/S + disclose in the app's privacy policy, which is easily viewed before any data is processed? ***Correct answer***

Key data privacy and security ("DP&S") dos and don'ts

Do *bake PBD and PIA into the process*

Don't *forget data security means taking* ***organisational*** *as well as technical measures*

Don't *be lazy about DP&S in supply agreements*

Do *focus on data flows and consent management*

Do *ensure pre-download notice and choice*

Don't *lose sight of privacy and electronic comms laws*

Don't *forget that for mobiles accessibility is key*

Guidance sources

- ICO Guide for App developers and mobile messaging
- Article 29 Working party opinion on apps and smart devices
- GSMA Mobile Privacy Principles
- MMA mobile application privacy policy guidelines
- …er….Osborne Clarke and of course
- www.marketinglaw.co.uk

Any questions?

Stephen Groom

Co-chair-Advertising & Marketing Law Group

Deputy Chair-Privacy and Data Law Group

T +44 (0) 207 105 7078

M +44 (0) 207 105 7078

stephen.groom@osborneclarke.com

www.marketinglaw.co.uk