SOCIAL LISTENING

Responding effectively to online insights

What is social listening?

Social listening involves monitoring social media to find out what is being said about you and your industry and using these insights to improve your business and engage with customers.



Producing personalised marketing materials

Producing personalised content based on an understanding of your customers. How does your target market converse, what words do they use? How can your target market be segmented into different categories?

Measuring marketing campaign success

Compare mentions of your products before and after the running of a campaign. Metrics for "impressions" or "views" alone can be unreliable.

Driving product development and innovation

See how customers respond to your products and products of your competitors. What features do they like? What don't they like? What products do they want to see?

Monitoring IPR infringement

Find out if your customers or potential customers are talking about a product which is a copy of your own

Improving customer service

Spotting trends in customer feedback and complaints in relation to you and your competitors, and identifying opportunities for prompt customer engagement. Social listening can create opportunities for interaction with customers who feel dissatisfied but have not communicated this to you directly.

What are the opportunities?

Crisis management

Track brand health in response to negative publicity to seek opportunities for remediation and mitigation.

Identifying customers, potential customers and influencers

Find out the best places to focus your marketing efforts and identify potential influencer relationships. Who is sharing information about your brand/industry? And where are they sharing

it?

Key legal and practical considerations

Data privacy

It's important to consider what data is collected and processed as part of any social listening campaign and, in particular, whether this will include personal data.

The use of personal data collected via social media is coming under increasing scrutiny following the implementation of the GDPR and the recent Facebook-Cambridge Analytica scandal. Where personal data is involved, think about the following key areas:

Data subject rights

You must have processes in place to ensure that you can fulfil any rights requests from data subjects (for example, who object to you using their data).

Transparency

How will you make users aware of how their scraped data will be used? The law generally requires you to provide a privacy notice, even where the data is from a third party source, unless a limited exemption applies.

Purpose

How is personal data used once collected?
Would individuals anticipate their data being used in this way and how will you ensure the data isn't used for additional unplanned purposes?

Data minimisation

Large scale trawling potentially conflicts with the requirement to hold only as much personal data as is required. How will you ensure that you only collect relevant data?

Anonymisation

Do you need to use personal data, or can wider trends being drawn from fully anonymised data? If you can use anonymous data, it is less risky.

Lawful basis

Do you have consent or another lawful basis for using personal data? Third party consents may be more difficult to rely on under the GDPR.

Retention and security

How long will personal data be retained for and how will it be destroyed?

How will you keep it safe?

Data scraping: Website operator objections

Social media website operators may object to data scraping to protect the value of data on their sites. The law surrounding the legality of data scraping and the rights of website operators is a complicated and developing area. Possible arguments include:

Website terms and conditions

Arguments based on breach of terms and conditions may be the most feasible argument for website operators in some circumstances, and it's common for website terms of use to prohibit data scraping. The key question is whether there is a valid contract incorporating the terms and conditions.

I.e. is there a passive set of website terms and conditions? Or is there a walled garden environment, whereby access to the database is conditional upon entering into access terms and conditions?





Copyright infringement

It would be difficult for social media website operators to bring copyright infringement claims, as proving that a "substantial part" of data was copied would be problematic. However, you should consider if users' copyright in content may be infringed.

Database Rights

The key issue for claims based on database rights will be whether database rights exist. Again, this would be tricky for social media website operators:

UK case law indicates that database rights are unlikely to arise where users generate content, rather than the website seeking content.





Other arguments

A question to be tested in the UK is whether data scraping could be a breach of the Computer Misuse Act 1990, which relates to hacking. Similar arguments have been brought in the US in relation to comparable legislation but, whilst the US courts have not taken a consistent approach, there seems to be an unwillingness to prohibit the harvesting of publicly available data on the basis of (old) anti-hacking legislation.



Service Provider terms

Make sure terms with social listening providers contain adequate protections, particularly in relation to the points discussed above. Key considerations include:





Data

0161 934 6329



020 7160 3297



020 7160 3178



addleshawgoddard.com

Aberdeen, Doha, Dubai, Edinburgh, Glasgow, Hong Kong, Leeds, London, Manchester, Muscat, Singapore and Tokyo* *a formal alliance with Hashidate Law Office

© 2018 Addleshaw Goddard LLP. All rights reserved. Extracts may be copied with prior permission and provided their source is acknowledged. This document is for general information only. It is not legal advice and should not be acted or relied on as being so, accordingly Addleshaw Goddard disclaims any responsibility. It does not create a solicitor-client relationship between Addleshaw Goddard and any other person. Legal advice should be taken before applying any information in this document to any facts and circumstances. Addleshaw Goddard is an international legal practice carried on by Addleshaw Goddard LLP (a limited liability partnership registered in England & Wales and authorised and regulated by the Solicitors Regulation Authority and the Law Society of Scotland) and its affiliated undertakings. Addleshaw Goddard operates in the Dubai International Financial Centre through Addleshaw Goddard (Middle East) LLP (registered with and regulated by the DFSA), in the Qatar Financial Centre through Addleshaw Goddard (GCC) LLP (licensed by the QFCA), in Oman through Addleshaw Goddard (Middle East) LLP in association with Nasser Al Habsi & Saif Al Mamari Law Firm (licensed by the Oman Ministry of Justice) and in Hong Kong, Addleshaw Goddard (Hong Kong) LLP, a Hong Kong limited liability partnership pursuant to the Legal Practitioners Ordinance and regulated by the Law Society of Hong Kong. In Tokyo, legal services are offered through Addleshaw Goddard's formal alliance with Hashidate Law Office. A list of members/principals for each firm will be provided upon request. The term partner refers to any individual who is a member of any Addleshaw Goddard entity or association or an employee or consultant with equivalent standing and qualifications. If you prefer not to receive promotional material from us, please email us at unsubscribe@addleshawgoddard.com. For further information please consult our website www.addleshawgoddard.com or www.aglaw.com.