Social Media, the GDPR and Data

18 Key Things You Need to Know

Responsible Marketing

DMA
Data & Marketing Association

Contents

Acknowledgements

The DMA would like to thank past and present members of the DMA Social Media Council for their contribution to this guide, in particular:

Laurier Nicas Alder, TMW Unlimited

Julie Atherton, Small Wonder

Sam Beament, Dyson

Milly Bellotti, Collider

Hannah Bland, Aviva Investors

Joel Davis, agency:2

Ben Dunham, Osborne Clarke

N**ick Joy,** LV=

Sally Rushton, Jaywing

Lynsey Sweales, Social B

Introduction

Social media can be the perfect tool for finding out what your consumers want from you and how they feel about your product. Don't let the GDPR make you afraid to handle your social media data.

The GDPR aims to put customers' personal data protection at the heart of every business.

With social media being used as a direct means of communication between business and consumer, it is important that you keep social media platforms secure and handle their personal data appropriately.

The DMA's Social Media Council have collated the key things you need to know about social media in relation to the GDPR.

The Council members have encountered these situations in their everyday work, and are sharing their experiences and knowledge to help you and your business.

Social media, the GDPR and data: 18 Things You Need to Know

1. Community Management

a) Public Messages

Personal data exchanged in public messages on social media platforms isn't owned by the brand or the agencies acting on behalf of brands; it is owned by the individual who uses social media platforms.

The social media platforms have their own privacy notices and guidelines which social media platform users and advertisers agree to comply with.

On top of this, brands must set out in their privacy notices how they will use such personal data in accordance with the requirements of the GDPR, in particular, but not exclusively, the right to be informed.

An example of this can be the Information Commissioner's Office's social media section in its privacy notice.

For further information on the right to be informed: click here.

When running a competition on a social media platform and collecting personal data for this purpose, competition entry terms and conditions must explain how the collected data will be used.

If a brand or an agency acting on behalf of a brand is moderating social media channels, then the staff members of the brand or agency working on behalf of the brand must carry out the moderation in line with the brand's social media policy.

The moderator may suggest to the social media user that it might be better to use direct messaging rather than public messaging when the user wishes to share his/her personal data.

If the user persists in sharing personal data via public messaging then in addition to the privacy notice; the moderator should use boilerplate clauses for public messages where personal data is disclosed, for example:

- Thank you for your message.
- We care about the security of our consumers, so please note that we will not use any of your personal details obtained in this communication for marketing purposes.

- If you provide us with any contact information for customer service purposes, it will only be used to manage your enquiry and will not be used for any other reason.
- Any personal data shared in public by the user on social platforms is shared at their own risk.

Social media users may not realise the consequences of sharing personal data on the platform via public messages and a brand cannot infer that a user has consented to the use of that personal data for any purpose.

Despite this, we'd recommend moderating the platforms to delete (where possible) any personal data that you believe that they have shared in error or without realising the consequences and/or encourage them to use direct messaging instead as explained above.

b) Private Messaging

The same points as in respect of public messaging are applicable to private messaging.

Brands or agencies acting on their behalf the brands should not do anything with personal data disclosed in private messages which the sender of that message would not expect.

2. B2B, B2C, and the GDPR

What are the differences between B2B and B2C sourced personal data?

The GDPR only applies to individuals' personal data and not to any information about organisations.

However, contact details of organisations' members (employees, contractors, consultants, trainees etc) such as name, job title, phone number, email address, and personal social media account details all fall within the definition of personal data.

The only exception to this applies to the use of generic email addresses such as sales@dma.org.uk: unless you know that an individual staff member has sole access to a generic email address.

If the individual member's details fall within the definition of personal data in the GDPR, then the organisation must process this information in accordance with the GDPR procedures and acknowledge that the member has all the data subject's rights under the GDPR.

The details of how many members the organisation has, its financial figures and postal address are not considered personal data.

3. B2B, Contact Data, and Prospect Purposes

A B2B website features their teams' direct email addresses and telephone numbers for enquiries; will this still be ok to use for prospect purposes under the GDPR?

In this situation, you would be allowed to use these contact details to contact the person if you were interested in using their services.

However, you would not be allowed to contact the person to sell your own services (as in cold contact). This would be seen as prospecting and using the data for purposes where no permission has been given by the individual concerned.

Using the provided information for any purpose other than that stated is prohibited under the GDPR.

It is still possible to contact the organisation to sell your services but the main contact number or general email address should be used as these are not considered to be personal data under GDPR.

4. Custom Audiences, Platforms, and the GDPR

How do you deal with custom audiences on social media platforms following GDPR?

A custom audience from a customer list is a type of audience that you can create on a social media platform made up of your existing customers.

In order to create the list, an advertiser must share customer data (usually email, but phone numbers can be used too) in order for the platform to match it with their database.

A crucial part of this process involves the scrambling or 'hashing' of data so it is obscured, but is still unique enough to be matched.

Once this information is matched, the advertiser will be able to target its customers on the list with adverts while they're using the platform.

Creating a custom audience can be extremely effective, especially if an advertiser segments their list prior to the upload.

In this case, the advertiser must state in their privacy notice that it will use the information it holds about its customers to find and contact them on social media platforms.

Facebook is introducing a Custom Audiences Permission Tool which will require advertisers to confirm that proper consent under the GDPR has been obtained for the personal data they upload to create custom audiences.

If a data privacy notice doesn't already include a statement that it will use information it already holds about them to find them on social media platforms, then the notice should be amended to include this information.

The data privacy notice must be updated in a language that can be easily understood, explaining how the data will be shared with social media platforms and that this will be done on the consent legal basis.

In addition, or alternatively, advertisers can use the data to create 'lookalikes', which will expand their audience exponentially to include people that display similar traits to the customers in the original upload.

In the case of creating lookalikes, there is no need for the advertiser to get the consent of its customers since the advertiser is not targeting them specifically.

The existing customers will be specifically excluded from the lookalike list.

What needs to be considered under the GDPR?

The handling of any personal data should always be taken seriously, especially as GDPR brings with it significant consequences for non-compliance, including fines of up to €20 million or 4% of a company's global turnover.

Organisations must have a legal basis for processing personal data under the GDPR and, as we have seen above, Facebook's new Custom Audiences Tool requires advertisers to obtain consent before uploading personal data to Facebook to create Custom Audiences.

In terms of the social media platforms using data to create lookalike audiences, they are able to do this based on the user's relationship with the platform.

The users will have agreed to receive lookalike advertisements when they signed up to the social media platform.

If a platform user responds to a lookalike advertisement, once the user goes back to the advertiser's website, the advertiser is responsible for compliance with the GDPR, in particular, the advertiser must make sure that it complies with the right to be informed under Article 13 of the GDPR.

[1] Reference – Articles 13 & 14 of the GDPR.

5. Retargeting Ads

Is it possible to use retargeting ads on social media platforms post the GDPR?

Retargeting allows you to serve adverts to people who have visited your website.

A pixel is placed on your website which is invisible to visitors and places a unique cookie in their browser which allows them to be identified as having visited your site.

Under the Privacy and Electronic Communications Regulations, you must obtain consent to use these types of cookies. Please click here for further information:

Please note that implied consent does not exist under the GDPR and you cannot use the legitimate interest legal ground under the GDPR for these types of cookies.

You will have to ensure that your consent for the use of retargeting cookies meets the GDPR standard of consent: Find out more here.

The current cookie law derives from a piece of European legislation called the ePrivacy Directive.

This is currently being revised and will become the ePrivacy Regulation, once it has completed its passage through the Brussels legislative process. We expect this to happen in late 2018 or early 2019.

There will almost certainly be major changes

6. Linking Social Channels

Can businesses link their social channels via email and their website under GDPR?

Yes, businesses will still be able to link to their social channels via email and their website and encourage people to connect with them on these platforms.

However, organisations will have to explain in their data privacy notice how they will use the social media contact information collected.

Organisations should also ensure that they have an internal social media policy detailing how members of the organisation will use and respond to social media sourced personal data.

7. Social Media and Superfans

If an organisation identifies a 'superfan' (customer), would this organisation be allowed to reach out to the superfan via social media touch points?

An organisation may be allowed to reach out to superfans via social media platforms in the following scenarios:

a) If the superfan is already a customer of the organisation

b) If the superfan is not already a customer of the organisation

If the superfan is already a customer of the organisation, then:

The organisation should have already given the superfan the required information under the right to be informed under the GDPR when they became a customer of the organisation.

The organisation must have told the superfan that it would send marketing messages and/or contact them via social media platforms.

In addition, the organisation would have to have a legal ground under the GDPR for reaching out to the superfan – the two most likely legal grounds are consent and legitimate interest.

If the superfan is not already a customer of the organisation, then:

The organisation will need to give the superfan the required information under the right to be informed under the GDPR.

The organisation would need to tell the superfan that it will contact them with marketing messages and/ or contact them via social media platforms.

In addition, the business would have to have a legal ground under the GDPR for reaching out to the superfan. The two most likely legal grounds are consent and legitimate interest.

8. Social Media Reporting and Storing

Social media reports are used to track performance against KPIs and provide insight for future campaign development.

Tracking performance

- Data for social media reports can come from a variety of sources including Google Analytics, in-app analytics or dedicated reporting tools. The data is usually held in a bespoke spreadsheet and is used to create a table or charts to highlight the results.

- Typical measures included in the reports are shares, likes, conversions, sales, engagement rates, reach, follows, clicks.

- As the data is held at an aggregated level it falls outside the definition of personal data in the GDPR and therefore this type of social media performance can continue to be reported in the same way post-GDPR.

Providing insight

- Social media reports can include example comments or screenshots of posts that provide insight on sentiment and opinion. These posts will fall within the definition of personal data in the GDPR but are publicly available to view on the social media platform.

- The posts can be included in a social media report post-GDPR as a link to the location on the social media platform.

- If a screenshot of the post or comment is included it should be anonymised.

- The advertiser will have to think carefully about the purpose for which it uses this personal data.

- For example, the advertiser cannot use the personal data in the post to send direct marketing to the platform user unless the platform user has already agreed to receive direct marketing from the advertiser.

9. Permissioning and Social Media

What is permissioning? How to permission or re-permission? What are the permissions in social media and how will they apply?

Organisations should have decided before the 25 May 2018 as to which legal ground under the GDPR they were going to use for their direct marketing activities.

There were six possible legal grounds under the GDPR and there is no hierarchy of legal grounds – an organisation just needs one legal ground.

The two most common legal grounds for direct marketing are consent and legitimate interest. For more information on these two grounds please see the DMA GDPR Guide here.

If brands are using the consent legal ground, they need to be aware of the **ICO** guidance advising that the consent should be revalidated once every two years under GDPR, showing an intention to ensure that consent isn't assumed to last for a long period.

Find out more here.

For the consent legal ground to work well, brands need to be more imaginative than they were with the cookie acceptance box, which offered no choice and frequently just got in the way.

Many are using the consent process more creatively, and so, instead of bluntly asking people if they want to consent to receive more communications, consent should be presented as an opportunity to engage with the brand confirming in the consumer's mind why they should consent.

Using the consent legal ground as the legal basis for direct marketing carries some risk including the risk of a complete opt-out from all channels because the recipient does not respond, low response rate etc.

The DMA advises organisations to consider using the legitimate interest legal ground as a basis for their direct marketing by postal mail to avoid the risk of a complete opt-out from all marketing channels because a customer does not respond to the request for consent.

The DMA would also advise organisations to carry out testing of the wording of consent requests to ensure they chose the wording which has the greatest response rate.

The exercise needs to be as user-friendly as possible to achieve the highest number of customers consenting to receive direct marketing whilst being conducted within the law.

What are permissions in social media and how do we apply them?

Thanks in part to the recent Cambridge Analytica case alongside GDPR, social media platforms have invited users to agree to new terms and conditions of use and also to review their individual user settings on the platform with regard to visibility to other platform users.

This in turn effects permissions for ad networks and the brands wanting to advertise on social media platforms either through paid (see our earlier notes on custom audiences) or organic activity.

For users of a social media platform who like or follow a brand's page on a platform, not much will change as as the user agrees prior to using the platform that they are happy to engage and be part of that brand's community on that platform.

However, if the brand wants to use the personal data collected via the platform to contact the user other than via the platform they will have to make this very clear in the brand's data privacy notice and find a legal ground under the GDPR for the use of this personal data.

Brands also need to be aware that the ePrivacy Directive is currently being revised and will become the ePrivacy Regulation.

It is currently going through the Brussels legislative process and is expected to be passed in late 2018 or early 2019.

It is not known at the moment when the new Regulation will come into force. One important point to note is that over the top services run by many social media platforms will come under the scope of the new Regulation.

10. Cybersecurity and Training

The obligations regarding the security of personal data held by a brand and cyber security have not really changed much under the GDPR.

The security principle in the GDPR requires organisations to process personal data securely by taking appropriate technical and organisational measures to protect personal data.

For more on the security principle please click here.

It is important that all staff members of an organisation are trained in data security measures appropriate to their job role. The Government Cyber Security Essentials website contains some good advice particularly for small organisations who may not have a dedicated IT security team.

If your organisation has an IT security team, then cybersecurity and training will be primarily their responsibility. All organisations – no matter what the size – should be aware of and should put the following basic cybersecurity items in place (this is not an exhaustive list):

- Storing all client/customer personal data and other confidential in a CRM system that is both secure and encrypted.
- All CRM and systems where personal data or other confidential information is stored must be password protected (passwords should be secure passwords – Click here for further info.
- Your network should be secure – there should be sufficient security and firewalls in place so that cyber-attacks can be limited, and, if there is a cyber-attack, its effects can be limited.
- You have anti-virus software installed / in place on every computer and device where your team accesses data.

As well as technical and organisational IT security all staff members should be trained to be 'cyber aware'.

Most cyber-attacks start with someone within an organisation replying to a cyber-attack phishing email – these emails will often appear to have been sent from a member of the senior management team of an organisation whose email account has been hacked/compromised.

If the email is opened or the attachment downloaded – the organisation could be exposed to a full-blown cyber-attack or ransomware attack.

To help limit the chances of this happening it's not only important that you have the correct security on emails in place, but also have your team trained.

Your team members need to follow the advice of your IT security team about using unsecured wifi networks (such as publicly available wifi networks in coffee shops and other places); what personal data and business confidential information you can transmit when using such networks; and any additional security measures staff members should take.

For more information, please click here.

It is important to review your cybersecurity within your organisation and upskill the level of cybersecurity knowledge with every staff member in your organisation.

These measures won't prevent a cyber-attack but they should limit the consequences of a cyber-attack.

11. Your Employee Advocates, the GDPR, and Social Media

Are there any particular GDPR considerations for our employee advocates using social media?

Absolutely, though there are not many changes from the way your employee advocates should have been using social media under the old data protection legislative framework.

Most of (if not all) your social media activity takes place on a third-party platform and the user will have already accepted the platform's data privacy notice and terms and conditions of use.

Their relationship is with the platform provider, not your organisation: members of an organisation who are social media advocates need to have a good working knowledge of each platforms' rules so they do not break them when they are promoting an organisation on a particular platform.

How personal data is presented or stored on a particular platform is the responsibility of the platform owner. Member advocates working on behalf of an organisation need to comply with the organisation's social media policy.

Member advocates need to have GDPR training so that they know that if the organisation they are working on behalf of takes some personal data from a social media platform, and it uses such information on its own account then the organisation – not the social media platform – will become the controller and be responsible for GDPR compliance.

For example, if we were to take some personal data from a Twitter post and store it in a spreadsheet or in an email then we would be liable for making sure that the personal information was being stored securely, was accurate, and held for no longer than necessary to achieve the purposes.

The organisation would also have to find one of the six legal grounds under the GDPR as its lawful basis for processing the personal data and then give the author of the Twitter post the required information under Article 14 of the GDPR.

12. Collecting Personal Data via Lead Generation

Will you still be able to collect personal data via lead generation forms (including third-party forms, i.e. Twitter cards)?

a) Twitter cards

Yes, you will.

The brand who has posted the Twitter card will still be able to get access to information about who has clicked on it through Twitter based on the platform's data privacy notice and terms and conditions.

However, if the call to action in the Twitter card is to direct users to click on a link to your website, when they land on your website and if you are using cookies, you will need to explain this on your website and depending on what you are using the cookies for, either get consent or use the legitimate interest legal ground under the GDPR.

Organisations must have a legal basis for processing personal data under the GDPR. If you are collecting personal data on the website then you will need to explain to visitors the purposes for which you are collecting the information.

GDPR legislation stipulates that personal data must be collected for "specified, explicit and legitimate purposes". Therefore, when personal data is collected, website owners must first explain to visitors how it will be used and provide them with their information rights, and secondly ensure the different purposes for processing the personal data are separated out.

Regarding the first point, it's up to the website owner to specify in the data collection form in what way the personal data will be used and ensure it is not ambiguous so for example instead of saying "marketing purposes", using wording such as "information and deals on new and current products".

On the question of separating consent for different purposes, website owners need to ensure that they are not grouping different purposes in one place so that users are able to select one purpose but not the other.

b) Third-party lead generation forms

You will still be able to collect personal data via third-party lead generation forms under the GDPR.

However, if you are collecting email addresses, mobile numbers for mobile marketing or social media handles to pass on to third parties, the lead generation company collecting the information can only do this using the consent legal ground under the GDPR.

The lead generation company will also have to name the third parties it wants to pass the information on to individually by name.

Organisations need to remember that consent to pass information on to third-parties is a one-step process. So the third-party who has received the personal data from the lead generation company cannot rely on the original consent given to the lead generation company for the third party to pass the personal data on to other third parties.

The third-party will need to carry out the due diligence on whether the lead generation company has correctly collected the personal data using the checklist in the **ICO** Direct Marketing Guidance for buying a marketing list in the Lead Generation and Marketing list section here.

If you are a first-party collecting personal data from a customer and want to pass it on to third-parties for lead generation then you must separate out the two purposes of first-party marketing and third-party marketing.

In addition, you must comply with all the other requirements of the GDPR outlined here.

13. The Right to be Forgotten

The GDPR grants various rights to data subjects.

One of these is the right to request erasure of their personal data, also known as the right to be forgotten.

The right is not absolute – it can only be exercised in certain situations.

See the **ICO** Guide to the GDPR on the right to erasure here.

14. Running Multi-national Campaigns under the GDPR

If an organisation runs a multi-national campaign from the UK to countries outside the EU, would it be correct that this wouldn't sit within the scope of the GDPR?

Organisations carrying out ad campaigns should be aware of the importance of complying with the GDPR insofar as the campaign will involve the collection, storing and/or use of personal data which identifies an individual.

However, one common misconception is to do with the applicability of the GDPR when organisations based in the UK run multi-national campaigns which collect the personal data of individuals based outside the EU.

The GDPR applies to "the activities of an establishment of a controller or processor in the Union".

In other words, the deciding factor is whether the party running the campaign is based in the EU, not the location of the data subjects. If the social campaign is being arranged from the UK by a UK brand (or a UK subsidiary of a global brand), all personal data processed as part of that campaign will need to be treated in compliance with the GDPR, even if the campaign is targeted at individuals in, say, Australia.

As such, the usual GDPR considerations such as having a lawful basis for processing personal data, ensuring appropriate security mechanisms are in place and transferring personal data outside the European Economic Area (EEA means the 28 Member States of the EU plus Iceland, Lichtenstein and Norway) only when recognised protections are in place will apply to any personal data obtained as part of the social campaign.

Of course, if the campaign is such that no personal data is processed by the brand running it then the GDPR would not apply in any event (such as targeted banner ads served using a social media site's own targeting capabilities where the brand does not come into contact with, or take ownership of, end user data).

In some ways, this can make things simpler for advertisers.

Rather than having to treat different personal data sets from social campaigns differently, depending on the location of the target audience, a uniform worldwide policy can be adopted which meets the GDPR standard.

That said, advertisers should also be aware that the use of personal data relating to an individual in a country outside the EU may also engage that country's own data protection laws.

As such, it is worth carrying out a local assessment in each case to check that the GDPR-compliant measures in place are sufficient to adhere to the relevant local rules.

15. Celebrity and Brand Accounts

If a business wants to work with celebrity and brand accounts on campaigns to reach their audiences, will any new factors need to be taken in to account for running these campaigns under the GDPR?

Unless you are asking for any personal details from the audiences – such as email or phone number – the rules for celebrity/brand relationships remains the same under GDPR.

This includes clear labelling of sponsored posts so that audiences are aware that it is a paid promotion.

If you are running a competition with an influencer or celebrity in which you require personal details from entrants, whether at entry stage or to contact winners, you need to ensure any handling of this data is GDPR-compliant.

Further details on competition handling can be found in Question 1 concerning competition draws.

The rules for celebrity brand relationships are part of the CAP Code and guidance can be found here.

16. Social Media Reports: Retaining and Using Data

What sort of data from social media reports can we retain and use, considering that it has been generated from a third-party platform?

As discussed, the processing of personal data that takes place on a social media platform is ultimately the responsibility of the platform provider.

They will have required users to sign up to their terms and conditions of use and their data privacy notice.

If the user agrees to these terms and conditions of use, and the data privacy notice, then it's up to that platform owner to ensure that the personal data held on the platform is processed in compliance with the GDPR.

However, the situation changes when a brand or agency acting on behalf of a brand uses a software tool to interrogate the platform(s) to extract personal information.

By removing that personal data from the original platform on which it was published, the responsibility shifts to us as we become controllers.

Accordingly, we have to treat that personal data in the same ways as any other personal data under the GDPR.

Ultimately you will have to comply with all the legal requirements under the GDPR including but not limited to making sure you have a legal ground under the GDPR for processing such personal data; a valid purpose as to why you are retrieving the personal data from the social media platform; and being able to justify your actions under the accountability principle.

If you are storing the personal data, you need to ensure it is accurate and kept up to date.

You must only keep the personal data for as long as it is necessary for the specified purposes.

As an example, you might run a report every month using your social media monitoring tool to measure sentiment. In this case, it's fine to run the report so that you can aggregate the total results (as this isn't giving away personal information).

If you export a spreadsheet with all the posts on it from a social media platform on it (highly likely to contain personal info), ask how you'll store it: do you really need it at all?

17. Running a Competition

Will competition draws such as 'like a page', 'like this post and share with your friends', and 'tag a friend' be allowed to be to run under the GDPR?

The way you run competitions using 'like a page' or 'like this post' doesn't need to change if you adhere to the platforms' terms and conditions.

You should bear in mind CAP's concerns about using these methods, which you can find here.

It is doubtful whether you will be able to use 'share with your friends' and 'tag a friend' as an entry mechanic for competition draws because of the higher consent standard under the GDPR.

It would be difficult for the promoter of the prize draw or competition to argue that the person referred or tagged had consented to receive marketing messages from the promoter.

You will have to ensure that how you collect and process personal data collected during entry to the prize draw/competition is compliant with the GDPR.

You will have to ensure that entrants are given the required information under the GDPR which you can find here.

The promoter will also have to ensure that they meet their accountability requirements under the GDPR and have appropriate policies and procedures in place such as data retention.

18. Dark Social and the GDPR

Is there anything an organisation needs to bear in mind on dark social going forward?

Dark social describes the social sharing of content that occurs outside of what can be measured.

By web analytics programmes, this occurs when a link is sent via online chat or email rather than via a social media platform – i.e. Techopedia.

Referrals from dark social are counted as direct traffic and this makes it difficult to measure social media as a whole.

This will remain unchanged under the GDPR as the referral source is anonymous.

About the Campaign

Responsible Marketing

Changes to the governance of data have far-reaching consequences for your business.

The new General Data Protection Regulations (GDPR) has already had an effect on how your business does business, and how it manages, protects and administers data in the future.

The new regulations came into place in 2018 and are still making waves.

At the DMA, we want to demystify these regulations and offer support to help you work to the best of your ability.

We also run events to encourage the practice of Responsible Marketing. Our popular Legal Updates discuss the current political and legal affairs affecting the industry and allow you to speak directly with the DMA's finest legal minds. Keep an eye on your emails, or visit our events page to book your spot.

For those dealing with vulnerable consumers, we have a masterclass in recognising the needs of vulnerable consumers and how to make reasonable adjustments to benefit a broad range of employees working with customers in vulnerable circumstances.

Find help and guidance for all matters regarding responsible marketing on the DMA site.

About the DMA

The Data & Marketing Association (DMA) comprises the DMA, Institute of Data & Marketing (IDM) and DMA Talent.

We seek to guide and inspire industry leaders; to advance careers; and to nurture the next generation of aspiring marketers.

We champion the way things should be done, through a rich fusion of technology, diverse talent, creativity, insight – underpinned by our customer-focussed principles.

We set the standards marketers must meet in order to thrive, representing over 1,000 members drawn from the UK's data and marketing landscape.

By working responsibly, sustainably and creatively, together we will drive the data and marketing industry forward to meet the needs of people today and tomorrow.

www.dma.org.uk

Copyright and Disclaimer