The University of Sheffield
Research Ethics Policy Note no. 14

RESEARCH INVOLVING SOCIAL MEDIA DATA

1. BACKGROUND

Social media are communication tools that allow users to share information and communicate online. The content they create may be publicly available, or access may be restricted to specific individuals or members of a group or community. Examples of social media platforms include Facebook, Twitter, Weibo, blogging sites (e.g. Wordpress), video sites (e.g. Youtube), online messaging services (e.g. Whatsapp), online dating services (e.g. OK Cupid, Grindr), discussion forums etc.

The data generated by users of these tools is a rich data source that is used by researchers across sectors. Social media data includes:

- content users create (e.g. a comment, Tweet, video, blog post etc)
- data that records users' engagement with content and other users (e.g. likes, shares, retweets, followers, friends etc)
- other user data that is collected by the social media company possibly without the user being aware e.g. location data.

Depending upon the nature of the research, social media data might be used for different purposes e.g.

- Observing social media users to gain insight into a social or socio-technical phenomenon
- Using social media data to develop and test a new tool e.g. a new interface for visualising social media content related to a particular topic

In all cases where social media data is being used for research purposes, ethical approval must be gained prior to collecting and analysing data.

Social media users are defined as **human participants** if you are observing them or using their data for research purposes

Most social media data is defined as **personally identifiable data** under the General Data Protection Regulation.

Due to the complex and evolving nature of social media platforms, it is not possible - or desirable – to provide strict rules regarding the ethical use of social media data. However, a number of organisations and networks have published more general guidelines and frameworks for assessing the ethical issues related to research using social media data which the UREC recommends for further reading. For example:

- AOIR Association of Internet Researchers (2012). Ethical decision-making and Internet research 2.0: Recommendations from the AoIR ethics working committee. Available at: http://aoir.org/reports/ethics2.pdf
- British Psychological Association (2013). Ethics Guidelines for internet-mediated research. Available at: http://www.bps.org.uk/system/files/Public%20files/inf206-guidelines-for-internet-mediated-research.pdf

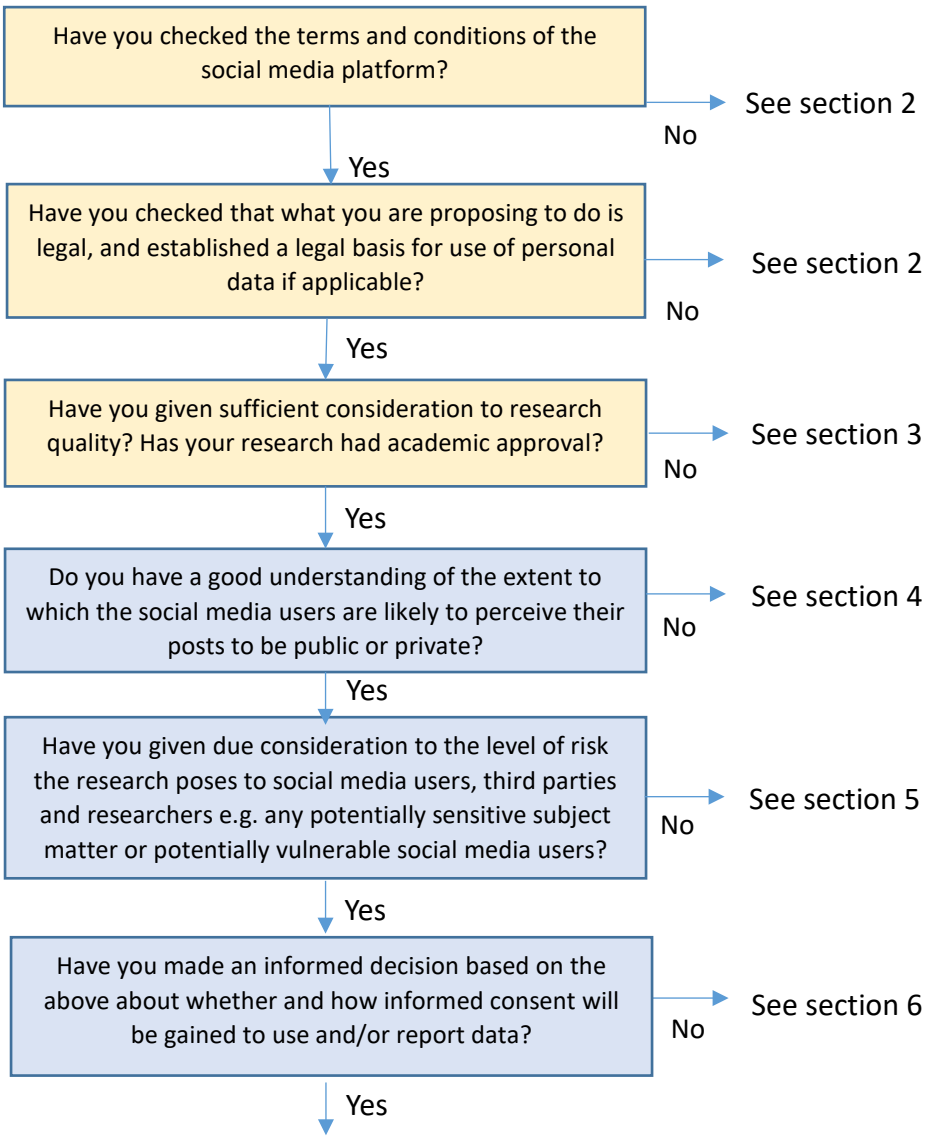
- ESRC (n.d.) Internet-mediated research. Available at: http://www.esrc.ac.uk/funding/guidance-for-applicants/research-ethics/frequently-raised-topics/internet-mediated-research/
- Townsend L. and Wallace C. (2016). Social Media Research: a guide to Ethics. Available at: www.dotrural.ac.uk/socialmediaresearchethics.pdf
- Zevenbergen. B et al (2016). Networked Systems Ethics. Available at: http://networkedsystemsethics.net/index.php?title=Networked_Systems_Ethics

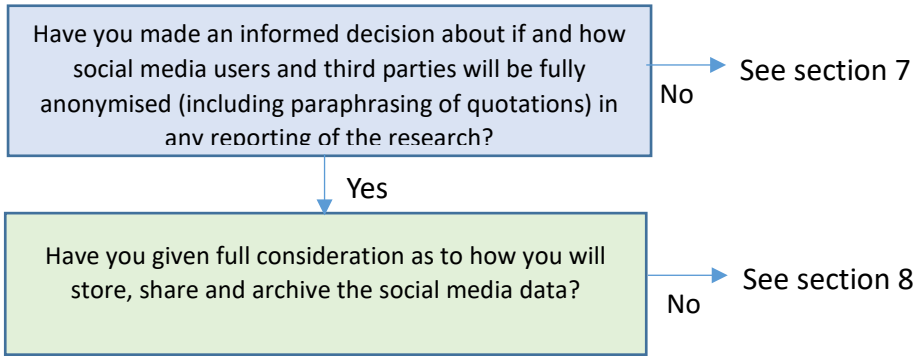
This policy note is based upon a review of these documents.

Ethical issues raised in four social media scenarios were also discussed in depth by participants in a UREC workshop (summer 2016). The scenarios and notes from these discussions are available on the UREC website, and aim to help generate thinking around the ethical issues related to social media research. http://www.sheffield.ac.uk/ris/other/gov-ethics/ethicspolicy/educationresources/social_media_workshop_july_16

There are many grey areas in social media research. Researchers should contact the UREC should they need advice on a specific research project.

Framework for addressing ethical considerations in social media research (Adapted from Townsend and Wallace, 2016)





2. IS IT LEGAL?

Before conducting any research using social media data it is important for the researcher to familiarise themselves with the Terms and Conditions of the social media platform, and make sure that what they are proposing to do is allowed by the site. Terms and Conditions of social media platforms change regularly, so researchers need to make sure that their understanding is up to date.

If using a third party tool to access social media data, the researcher should also ensure that the tool is compliant with the Terms and Conditions of the social media platform.

Other legal considerations include those related to

1) Data Protection (i.e. if you are storing and processing potentially identifiable social media data);

Social Media and the EU General Data Protection Regulation (GDPR) (NB. Other laws may apply to research undertaken outside the EU)

Identifiable and potentially identifiable social media data is subject to regulations set out in the GDPR, and an appropriate legal basis for the processing of personal data must be identified Social media data is still potentially identifiable even if user names have been removed.

Information Commissioner's Office (regulators of Data Protection in UK)

"There are many examples of big data analytics that do involve processing personal data, from **sources such as social media**....where personal data is being used, organisations must ensure they are complying with their obligations.

If personal data is fully anonymised, it is no longer personal data. In this context, **anonymised means that it is not possible to identify an individual from the data itself or from that data in combination with other data, taking account of all the means that are reasonably likely to be used to identify them**...The issue is not about eliminating the risk of re-identification altogether, but whether it can be mitigated so it is no longer significant...**Organisations using anonymised data need to be able demonstrate that they have carried out this robust assessment of the risk of re-identification**, and have adopted solutions proportionate to the risk."(ICO, 2014)

For more guidance on data protection obligations, and what an appropriate legal basis may be, refer to the Research Ethics Policy Note no. 4 'Principles of Anonymity, Confidentiality and Data Protection'

2) Intellectual Property (i.e. copyright on posts and images you may wish to reproduce).

3. IS IT HIGH QUALITY RESEARCH?

There are many tools available that allow for social media data to be quickly analysed and reported, without much consideration of research methods or integrity. Like all research conducted by staff and students of the University, social media research must meet standards of research quality and integrity appropriate to the discipline of the researcher.

Researchers are also advised to consider the methodological and ethical implications of using platforms and tools that do not enable the researcher's full understanding of the methods used to collect, analyse and report social media data.

Whilst this policy note only applies to use of social media data for research purposes (defined as "a process of investigation leading to new insights, effectively shared", some of the issues discussed may also be appropriate to consider for other non-research uses of social media data (e.g. marketing, public engagement etc).

4. ARE THE SOCIAL MEDIA POSTS PUBLIC OR PRIVATE?

A significant area of debate relates to whether social media posts should be classified as public or private.

Whether posts are perceived to be public or private impacts upon whether informed consent should be sought from social media users, however it has no impact upon whether ethical approval should be sought.

All research involving social media data must be ethically approved prior to data being collected and analysed.

As argued by the British Psychological Association (2013) whether a post should be perceived as public or private largely depends upon the specific online context, and – importantly – it is **the likely perception of the social media user** that is paramount.

Examples:

- Users of a 'private' Facebook group might reasonably expect that their posts are only visible to a restricted number of people and are therefore not 'public' – to enter the group without the knowledge or consent of moderators and/or users would be deception
- Twitter users using a #hashtag to make their Tweets more visible are more likely to consider their posts 'public'
- Users of a public discussion forum on a topic with limited general interest may reasonably expect that only a small number of people are likely to view the posts – they therefore may not perceive them as public

When assessing the public/private nature of online spaces it's important to take into account that people's perceptions vary, and not all social media users have a good understanding of how accessible their content is to others.

5. WHAT IS THE POTENTIAL FOR HARM AS A RESULT OF THE RESEARCH?

As with all research the potential vulnerability of participants and the sensitivity of the topic needs to be considered (see section 3.1.4 of the Ethics Review Procedure section of the Policy for potentially high risk topics and groups).

Researchers using social media are at a disadvantage in that they have no direct contact with the populations they are observing. It is therefore difficult to assess the potential vulnerability of participants. If you suspect that data originates from a potentially vulnerable user, including under 18s, the data should be removed from the dataset or appropriate measures should be put in place to gain appropriate informed consent for use of the data, including parental consent where appropriate (see Research Ethics Policy Note no.2 (Principles of Consent)). If engaging with participants online, where it may be difficult to establish the age of the participant, consideration should be given to steps that may be taken to verify the participants' age, and researchers must carefully consider the legal and ethical dimensions of involving participants under the age of 18.

Research involving sensitive topics, or topics with an increased likelihood of harvesting sensitive data, has a higher risk of causing harm to the social media users, people depicted in social media posts (e.g. people that are named, appear in photos etc), researchers and/or third parties. See section 3.1.4 of the Ethics Review Procedure section of the Policy for information about what classifies as a potentially sensitive topic. It should be noted that under the GDPR certain types of sensitive personal data are classified as 'special categories' of personal data and specific requirements apply when processing them; refer to the Specialist Research Ethics Guidance Paper on 'Anonymity, Confidentiality and Data Protection' for more details.

Inflammatory and offensive content is not uncommon on social media, and comments made in the heat of the moment may cause significant harm if they re-surface or are drawn attention to.

The potential of social media research to draw attention to posts and/or individuals that may otherwise have been lost in a crowd should be considered in relation to how such attention may risk harm.

As with all research, the sensitivity of the topic impacts upon ethical decision making, but in projects involving social media data special attention should be paid to how users interact with these platforms, how this may be different from interaction in a research setting or face to face, and what the implications are for conducting ethical research.

The timing of the research is also an issue to be considered in terms of the potential harm to participants. Researching 'live', current social media activity is likely to have a greater potential for harm; for example, due to a greater likelihood of individuals being identifiable, and a greater risk of altering the behaviour of the participants such as discouraging or changing their use of a particular social media platform. If a researcher intends to analyse current social media activity in their research, then their ethics application should address these issues thoroughly, including consideration of why it is necessary to research current, rather than inactive, discussions.

Some types of social media research involve collecting 'live' social media data as it is generated by users in response to particular types of events e.g. natural disasters, the specific details of which are unlikely to be known at the time of the ethics application. Due to the need to react quickly to live events, it may not be possible for the ethics application to be specific about the particular activity, but should indicate the type of events that the researcher intends to research, and give in depth consideration to the type of data that may be used, issues of

anomymisation, consent, risk and sensitivity, the type of analysis to be conducted, and when/how findings are to be published (i.e. immediate publication online; delayed publication in academic journal).

The higher the risk of potential harm the research poses, the more complex it becomes to address issues of appropriate consent and anonymisation, and the increased demand there is on the researcher to address these issues thoroughly.

6. IS INFORMED CONSENT REQUIRED?

Assuming consent is not being used as the legal basis for the processing of personal data according to the GDPR (in which case GDPR-compliant consent MUST be obtained), an assessment of the public/private nature of the post will impact upon whether informed consent should be sought and, if so, who from. As stated by the British Psychological Association (2013):

> "Where it is reasonable to argue that there is likely no perception and/or expectation of privacy (or where scientific/social value and/or research validity considerations are deemed to justify undisclosed observation), use of research data without gaining valid consent may be justifiable."

Whether informed consent is needed or not does not impact upon the need to get ethical approval. The ethics application should explain decision making with respect to whether or not to gain informed consent.

Observation of online public spaces

As with all research involving observation of public space it is recognised that it is often infeasible and unnecessary to gain the consent of all that may be observed. However, as stated in Research Ethics Policy Note no. 2 (Principles of Consent), if researchers are observing individuals in public places then unless consent is gained "specific individuals should not be identified, explicitly or by implication, in any reporting of the research, other than public figures acting in their public capacity (as in reporting a speech by a named individual, for example)". This aligns with recommendations in a number of social media research ethics guidelines. In such cases, if appropriate anonymisation is used (see section 7 below) then it may be appropriate to argue that consent is not required.

Observation of online spaces that may be perceived as not fully public by social media users

In cases where social media users may perceive their posts as not fully public, it may be necessary to gain appropriate consent. What is appropriate will depend on the nature of the research in question. For example, if the social media data is likely to be perceived by users as fairly public, the research is low risk, and the analysis is at the population level and no users will be identified, it may be appropriate to check that the terms and conditions of the platform state that the users have agreed to explicitly allow research use of data and/or to get consent from a gatekeeper (e.g. forum moderator, group administrator).

However, the less public the data, the higher risk the research and/or the more individual the analysis becomes, the more it will be necessary to consider how to gain informed consent from gatekeepers and/or individual social media users for:

1. Data harvesting and/or analysis;
2. Quoting or reproducing social media posts;
3. Identification of social media users in publications and tools.

Dependent upon the nature of the research it may be appropriate to get consent from gatekeepers and/or individual social media users for some or all of the above.

In making a decision about how to gain informed consent the following should be considered:

- Explicit statements on the website or in the terms and conditions of the platform
- The perspective of gatekeepers (e.g. forum moderators, group administrators) regarding the social media users' preferences about the use of their data
- The researcher's level of engagement with the social media users (i.e. will they observe/analyse data without interacting, or will they engage directly with users?) (see Research Ethics Policy Note no.2 (Principles of Consent) with respect to consent in participant observation (section 7) and the Specialist Research Ethics Guidance Paper entitled 'Ethical considerations in autoethnographic research')
- The potential harm to the community if they become aware of a researcher observing their interactions (see British Psychological Association (2013) Principle 3: Social Responsibility p. 6)
- Whether the nature of the research means that it is appropriate to engage in covert observation of a non-public space (see Policy Note no. 2 (Principles of Consent) with respect to research involving principled deception (section 6))
- How practically to gain consent from the appropriate people (e.g. could individuals be directed to a website that contains information about the research? Can consent be gained directly within the platform e.g. via a direct Tweet, Facebook message etc?)
- Should participants be offered the opportunity to consent (or not) to different things e.g.
    - Having their interactions observed;
    - Being identified in reports and publications;
    - Being directly quoted;
    - Having posts reproduced in publications.

Deleted posts

A significant issue arising in social media research is how to handle deleted posts. If the researcher collects their data before the post is deleted, the researcher may be unaware of the deletion and analyse it alongside other still existing data.

If a user deletes a comment this suggests they do not want others to see it, and this might be interpreted as equivalent to a request to withdraw consent for use of data (whether or not direct consent was obtained). It is therefore important to ensure that ethical decision making around reporting social media data takes into account such an eventuality whilst maintaining the integrity of the research, and that researchers consider what they will do if they become aware that there are deleted posts in their dataset.

Research by IPSOS MORI (2015) suggests that the public in general are uncomfortable with researchers' use of social media data.

Only 38% of respondents were aware that social media companies share individuals' social media data with third parties, such as the government or companies, for research purposes - and 60% of respondents believed this should not be happening.

Whilst the public were more favourable towards university researchers analysing social media data (more so than researchers based in government departments and companies), rates of acceptance were still low (approx. one third). Out of a number of scenarios presented to respondents, the one rated most favourably in terms of ethicality was still only deemed ethically acceptable by 50%. This scenario involved the following conditions being met:

- The researchers were based in a University or similar organisation
- They were only using the data of social media users who had **opted in to their data being used for this specific project**
- They were collecting data related to use of a specific word, hashtag or phrase relevant to the project
- The researchers were aiming to review or act on **comments about a product or service they deliver.**

(IPSOS MORI, 2015)

These findings suggest a lack of awareness and consent for academic use of social media data for research purposes, and challenge assumptions of implied informed consent to conduct research using social media data.

Whilst these findings should not necessarily stop social media research being conducted, they do suggest that issues of consent need to be thoroughly considered, and that ethical practice may also involve more open and public discussion about social media research methods, and the contribution that such research makes to society.

7. CONFIDENTIALITY AND ANONYMISATION

Unless a researcher seeks explicit consent from a social media user to identify them in the research, **steps should be taken to anonymise individuals in publications and other outputs, unless the individual is a public figure acting in a public capacity** (see Research Ethics Policy Note no.2 (Principles of Consent)). This is the case whether the social media data is perceived to be public or private. The need to anonymise applies both to individual social media users, as well as other individuals that they mention or depict in their posts.

In the case of photographs of people which have been shared on social media, the researcher should consider whether the person depicted has consented to their photograph been taken and shared. For example, for a stock image of a model, we can assume consent has been gained from the model for taking and reproducing the image – although the researcher may need to check whether the image is protected by copyright. On the other hand, in the case of a photograph of an individual taking part in a protest, we cannot assume the individual has consented to the image being taken and shared, and furthermore its reproduction could cause harm to the individual in some social contexts.

How to anonymise social media data

- The researchers should only collect the identifying information that they need to do the research (is the collection of usernames, profile descriptions, profile photos, date of birth, location etc. really necessary?).
- The researcher should consider replacing identifying information (e.g. usernames) at the earliest opportunity. Remember that such datasets are often re-identifiable using the correct techniques, so they should still be treated as though they were identifiable data, and in line with the GDPR
- If potentially identifying information (e.g. usernames, locations) needs to be retained in order to conduct the analysis then, unless the researcher has gained consent to identify users in reports, in most cases users should be anonymised in the reporting of research e.g. by using pseudonyms and image editing software such as Photoshop to hide identifying information and images in screenshots.
- Beyond using pseudonyms and removing identifying information, it is also recommended that if the researcher wants to report direct quotations that they paraphrase the quotation in a way that retains meaning. For higher risk research this should be standard practice. Advice on anonymization practices can be found here (British Psychological Society, 2013 p. 18; Townsend and Wallace, 2016, pp. 11-12). Paraphrasing is used because it is fairly easy to trace the source of direct quotations using a search engine.

Anonymization practices sometimes go against the Terms and Conditions of some platforms e.g. Twitter states Tweets must be given in their original form and attributed to the individual who posted the Tweet. In such cases careful consideration needs to be given as to what is ethically appropriate.

8. DATA STORAGE, SHARING AND RE-USE

As with all research consideration needs to be given to how to store, share and archive social media datasets. As discussed above, potentially identifiable social media data is regulated under the GDPR, and researchers are advised to follow University of Sheffield Research Data Management guidelines in relation to handling such data. The terms and conditions of the relevant social media platform, and if relevant commercial data provider, should also be checked for requirements relating to data storage, sharing and archiving. In the case of contradictory demands, advice can be sought from UREC.

Some social media data providers allow researchers to analyse data online, rather than needing to download and store it themselves. If these tools are provided legally and in line with the terms and conditions of the social media platform, they may be a suitable alternative to downloading and storing data. However, such tools are not always transparent in relation to how data are collected, analysed and presented, which can raise separate research integrity and ethical issues as discussed in section 3 above.

References

British Psychological Association (2013). Ethics Guidelines for internet-mediated research. Available at: http://www.bps.org.uk/system/files/Public%20files/inf206-guidelines-for-internet-mediated-research.pdf

ICO (2014), Big Data and Data Protection. Available at: https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf

IPSOS MORI (2015) #SocialEthics: A guide to embedding ethics in social media research. Available at: https://www.ipsos-mori.com/researchpublications/publications/1771/Ipsos-MORI-and-DemosCASM-call-for-better-ethical-standards-in-social-media-research.aspx

Townsend L. and Wallace C. (2016). Social Media Research: a guide to Ethics. Available at: www.dotrural.ac.uk/socialmediaresearchethics.pdf