HALLVARD FOSSHEIM | HELENE INGIERD (EDS.)

INTERNET RESEARCH ETHICS

DAG ELGESEM | BERNARD ENJOLRAS | CHARLES ESS
ANDERS OLOF LARSSON | MARIKA LÜDERS
ROBRINDRA PRABHU | KATRINE SEGADAL
ELISABETH STAKSRUD | KARI STEEN-JOHNSEN

CAPPELEN DAMM AKADEMISK

Internet research ethics

Hallvard Fossheim and Helene Ingierd (eds.)

Internet research ethics

CAPPELEN DAMM
AKADEMISK

This book was first published 2015 by Cappelen Damm Akademisk.

ISBN: 978-82-02-48035-6 Printed Edition

www.cda.no

This book has been published in cooperation with The Norwegian National Committees for Research Ethics.

ISBN: 978-82-02-48951-9 E-PDF

Typesetting: Datapage India (Pvt.) Ltd.
Cover Design: Kristin Berg Johnsen

noasp@cappelendamm.no

Table of contents

Introductory remarks

Hallvard Fossheim and Helene Ingierd
The Norwegian National Committees for Research Ethics

«Internet research» does not make up one unified object. The term denotes a wide array of research on Internet activities and structures, as well as research that utilizes the Internet as a source of data or even of processing. There is still good reason to make Internet research the unifying topic of an ethical treatment, however, for many forms of Internet research confront us with the same or similar ethical challenges.

In a given Internet research project, there is sometimes real worry or disagreement about what will constitute the best solution from an ethical point of view. It is relevant to this state of affairs that the relative novelty of the technology and practices involved can sometimes make it difficult to see when two cases are ethically similar in a relevant way and when they are not. Similarly, it is not always entirely clear whether and to what extent we may transfer our experiences from other areas of research to Internet research. In some respects, Internet research seems to be part of a broader technological development that confronts us with substantially new challenges, and to the extent that this is true, there will be less of a well-established practice on how to handle them. Some of these challenges also seem to apply to the judicial sphere when it comes to formulating and interpreting relevant laws.

To provide something by way of a very rough sketch of the sort of issues that confront us, many of the ethically relevant questions

voiced about Internet research concern personal information, and are posed in terms of access, protection, ownership, or validity. These questions are especially relevant when the research concerns what is often referred to as Big Data, our amassed digital traces constituting enormous data sets available to others. The fact that much of this information has been created and spread willingly generates complex questions about degrees of legitimacy for the researcher who chooses to appropriate and recontextualize that information, sometimes also with the potential of re-identification through purportedly anonymized data. The issues are naturally made even more complex in cases of third person information, or where the individual is a child or young person.

Person-related information that is available online to researchers (and others) covers the entire spectrum from the trivial and commonly known to the deeply sensitive and personal. Along another ethically relevant axis, one encounters information that is openly available to anyone interested at one extreme, and information that is protected by access restrictions or encryption at the other extreme.

There is also the question of the impact that research can have on the object of research, i.e., whether there is a risk of harm to participants, and whether and to what extent one should demand that the research constitutes a good to others besides the researcher. This is a feature shared by all research on human beings. But in the case of Internet research, it is often the case that the impact (and the importance of the impact) are particularly difficult to foresee; think, e.g., of how research on an individual or a group online can affect those people's behavior, either as a direct consequence of the researcher's presence or as an indirect consequence of the publication of the results.

Moreover, in much Internet research, the data that is collected, systematized, and interpreted is generated in contexts other than

those of research. Questions arise as to when exceptions from consent are justified, as well as to how consent may be obtained in a voluntary and informed manner in an online setting. In research on or with human beings, voluntary informed consent constitutes a sort of gold standard, deviations from which in most contexts require special justification. While the requirement of voluntary informed consent is grounded in respect for research subjects, a related strategy for ensuring ethically responsible practice in cases where consent might not be required is to take steps to inform the relevant persons about the research that is carried out.

Finally, it bears mention that ten years ago, there was precious little hint of how important social media would be today, and it is as difficult – i.e., impossible – for us to predict what might appear on our online horizon in the coming years. So while sorting out the ethically salient differences between practices and platforms is of great importance for finding responsible ethical solutions, we should also keep in mind the importance of realizing that both habits and technology can change the premises of the discussion swiftly and dramatically.

*

In his contribution, *Dag Elgesem* discusses research on social media and the requirements relating to information and consent. With regard to the requirement of consent, he argues that there is a crucial distinction between a situation in which participating in the research entails a risk of harm, and a situation in which there is no such risk, but the research challenges the individual's control over information about herself.

As Internet research evolves, there is also a great need for knowledge about the legal requirements related to using the Internet as a data source. In her contribution, *Katrine Segadal* gives an overview of the key legal documents regulating this area of research. While

the main rule is that that the processing of personal information should be based on informed consent, this is not a rule without important exceptions.

Charles Ess focuses on how our understandings of human selfhood and identity have begun to shift towards relational conceptions. These shifts are accompanied, he points out, by changing conceptions regarding morality and responsibility. For example, the obligation to protect privacy is not only an obligation vis-à-vis the individual, but also an obligation towards groups.

Marika Lüders discusses research on online practices, using two examples from her own research. Even though there is a potential public character of the content and people being studied, this does not warrant the public display and exposure of the research subjects, she argues. She holds that traditional research ethics, securing the privacy of the research subject, remains a key obligation, and so a primary challenge is how to conduct this type of research without compromising the individuals being studied.

Elisabeth Staksrud addresses pressing questions raised by research on children's online communication. She highlights the importance of including children when researching online environments. Drawing on examples, she provides input as to how this aim may be accomplished in a responsible manner.

Kari Steen-Johansen and *Bernard Enjolras* focus on the use of Big Data in research. Recognizing that Big Data presents researchers with new opportunities for analyzing social phenomena, they also stress how such data has its limitations and introduces a set of new ethical and practical challenges, not least related to how ownership and access to data are regulated.

Anders Olof Larsson deals with ethical and methodological challenges arising when gathering masses of data from social media services, such as Twitter and Facebook. Besides articulating a related range of difficulties having to do with discerning ethically

salient differences from one form of social media service to another, Larsson also discusses how differences in access among researchers might constitute a problem in its own right.

Robindra Prabhu makes the point that while we should attend to the pressing concerns relating to privacy and integrity that are raised by Big Data, we should not lose sight of the many issues that fall outside the traditional privacy debate relating to the effects the use of these data may have on human activities. He argues that these new challenges will require strong governance and legal protections.

Consent and information – ethical considerations when conducting research on social media

Dag Elgesem

Department of Information Science and
Media Studies, University of Bergen
Dag.Elgesem@infomedia.uib.no

Introduction

My topic is research on social media and the requirements regarding information and consent arising from such research. This article will primarily discuss the responsibility of researchers for giving due consideration to their research participants. It is also important to remember, however, that the value of the research is an ethical consideration that must be given weight, as the Norwegian National Committees for Research Ethics (NESH) points out in its guidelines on Internet research (NESH, 2003, point 1):

> Research on the Internet is valuable both because it can generate insight into a new and important communication channel and because the Internet provides the opportunity to study known

phenomena (e.g. formation of norms, dissemination of information, communication, formation of groups) in new ways.

The requirements regarding information and consent when conducting research on social media are not essentially different from other research involving people's participation. However, research is conducted in contexts that are structured by technologies and in which the conditions for communication are not always as clear or known for everyone involved. This applies in particular to the boundaries between the public and private spheres, which are often drawn in new ways and which therefore cause us in some cases to be uncertain about which requirements regarding information and consent should apply. But not everything is equally unclear. In cases where a service is both password protected and entails sensitive information, such as a personal Facebook profile, it seems obvious that the usual requirements regarding consent must apply. In contrast, I argue in this chapter that there are weaker grounds for obtaining consent to use non-private information that individuals themselves have made available in a public forum, such as postings about political issues in debate forums in online newspapers or on Twitter. I argue that in some cases research on social media is ethically responsible without consent and that the interests of those involved may be safeguarded in other ways.

Consent

A useful starting point for this discussion is the model developed by McKee and Porter (2009, p. 88), shown in Figure 1 below, which identifies four factors that affect the need to obtain consent when research is conducted on and outside of the Internet: degree of accessibility in the public sphere, sensitivity of the information, degree of interaction with the research participants and the vulnerability of the research participants.

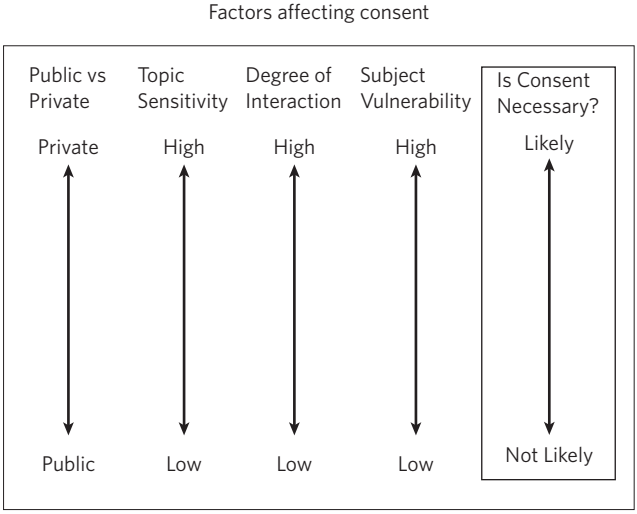

Figure 1 Factors affecting the requirement regarding consent (McKee and Porter, 2009, p. 88)

McKee and Porter's model identifies some of the sources of the uncertainty surrounding the requirements regarding consent when conducting research on social media: the ethically relevant factors (public versus private, sensitivity, interaction, vulnerability) are present in varying degrees and may occur in various combinations. It is therefore difficult to formulate simple, general rules, and on this basis McKee and Porter recommend a case-based approach with concrete assessments of the ethical issues raised by various research projects.

It is clear that the four factors affecting requirements regarding consent in McKee and Porter's model are not unique to research on the Internet, but are relevant in all research on communication. However, what complicates matters is that the boundaries between the private and public spheres appear in new ways, and the technological context creates new forms of interaction. This means that our ethical intuition about how we should regard these aspects is less clear.

In a number of often cited works, danah boyd has identified some properties of what she calls the «networked public sphere», which give communication on the Internet a character different from communication in other channels (boyd, 2008, p. 26 ff):

- *Persistence*: postings on the Internet are automatically registered and stored;
- *Replicability*: content in digital form can be duplicated without cost;
- *Invisible audiences*: we do not know who sees our postings.
- *Searchability*: content in the networked public sphere is very easily accessible by conducting a search.

These are interesting and important observations of some of the special features of Internet communication, which also shed light on why issues related to consent in research on the Internet may be more difficult to assess than other types of research. For example, since it may be unclear who the audience is for postings on the public sphere of the Internet, it is also more unclear who the postings in this sphere are intended for, and thus it is more difficult to assess whether the use of communication in research conflicts with this intention. The question is whether or not the use of information is related to a purpose different from the original one. A clear «yes» to this question will normally result in a requirement to obtain consent. The problem is that there is no clear delimitation of the target in much of the communication on the Internet because the intended audience is not restricted by the context of the communication. Examples of postings in which the audience is «invisible» and not clearly defined are replies in a comment field in an online newspaper, a Twitter post or an article in a blog. Below I return to the question of which role consent should play in research on media with an invisible audience.

By the same token, not all communication on the Internet has all of these properties to the same degree. Not all Facebook content is searchable by everyone, and we know who the audience is for the comments we post there (if we have set our privacy settings correctly). Often the ethical requirements regarding research will be stricter when the communication does not have the four properties identified by boyd because this communication is more private.

I share McKee and Porter's view that it is difficult to give simple, general rules for assessing when the requirement regarding consent should apply, and that it is necessary to make concrete assessments on a case-by-case basis. However, I will argue that there is an ethically relevant distinction between situations in which participating in the research entails a risk of harm or discomfort and those in which there is no such risk but the research nonetheless challenges the individual's interest in retaining control over information about himself/herself. Although the boundary here is fluid, and breaches of personal privacy are of course burdensome, I believe the two situations are different in ethically relevant ways. In the first case, there must be a *requirement* to obtain consent, whereas information and consent in the other type of situation is an important *consideration*, which in some cases may be weighed against other considerations. I will argue that research on certain types of communication on social media, such as political postings on Twitter, may be conducted without obtaining consent.

Situations in which there is a risk of discomfort or harm trigger an unconditional requirement to obtain consent: It must be up to the potential research participant to decide whether to subject himself/herself to the relevant risk or discomfort. As mentioned in the introduction, I believe that assessments related to the value of the research and its quality are relevant considerations in an ethical assessment, but in situations in which there is a risk of discomfort or harm, the

consideration given to the value of the research will not diminish the requirement to obtain consent. My view – and I think I am in line with the NESH guidelines – is that if it is not possible to obtain participants' consent in projects that entail such risk, the research cannot be carried out. Allow me to illustrate this point with an example:

Example 1: Research on Internet dating services

A group of economists in one of Norway's neighbouring countries wanted to study preference patterns of partner selection on Internet dating sites. Simply explained, the researchers created fictional profiles on the dating site, some of women and some of men. The profiles had some similar features, but were different with regard to income, education and ethnicity. The researchers wanted to find out what difference these features made in the market for partners. For each variable the researchers planned to contact a random sample of (real) persons on the dating site and register the features of the profiles of those who responded and those who did not. After the data was collected, the researchers would tell those who had answered the inquiries that they were no longer interested.

The project, which as far as I know was never carried out,[1] aimed to shed light on an increasingly popular phenomenon in the social network which provides new ways of finding a partner with consequences we know very little about. The methodological design of the project also seemed to be well planned. But this could hardly make up for the project's ethical problems. Firstly, the project had a hidden agenda in which it was essential that those involved did not know the real purpose of the inquiries. They did not even know that they were objects of research. Moreover, people who post a profile

1 Personal communication.

on a dating site are in a vulnerable situation, and the research activity may trigger burdensome emotional processes resulting from dashed hopes and disappointment. So although it could be argued that a project like this is interesting and increases insight into an important phenomenon, consideration towards the people who are the object of the research indicates that the project should not be carried out in this form.

Retaining control over one's own information

Ethical challenges related to personal privacy arise when the research infringes on the individual's interest in retaining control of information about himself/herself. The problem here is not necessarily that the research may be burdensome, as in the example above, but whether the research shows reasonable respect for the individual's integrity and interest in retaining control of his/her own information. Respect for personal privacy indicates that consent to use information about an individual in a research project should normally be obtained, although I will argue that this consideration is weaker than the requirement to avoid the risk of harm and discomfort.

In situations where the research will challenge the individual's interest in retaining control of information about himself/herself, this interest should normally be protected through consent obtained by the researcher. By the same token, I believe there are situations, especially when consent is very difficult to obtain, in which consideration for the value of the research may make it defensible to implement the project without consent. I return to this matter below. But let us first look at an example of research on social media that is clearly problematic from the perspective of personal privacy.

Example 2: Research on Facebook[2]

In 2008, US researchers made the Facebook profiles of an entire class of students from an unidentified US college available on the Internet. The dataset contained 1,700 profiles from the students' first academic year in 2006. Comparable data were also collected from the two subsequent years, which were planned to be published at a later time. Making the data publicly available was done in accordance with requirements imposed by the project's public funding source to allow other researchers to reuse the data.

The data was collected by research assistants who were also members of the Facebook network, but the other students had not given their consent to the use of the information in the research project. However, the information was made less identifiable and less sensitive before it was published by deleting the students' names and identification numbers and removing the most sensitive information about their interests. Thus the information published was not directly identifiable, and it could only be used for statistical purposes.

The researcher responsible for the project defended the project on the grounds that the research would not entail a risk or burden for the people involved. «We have not accessed any information not otherwise available on Facebook. We have not interviewed anyone, nor asked them for any information, nor made information about them public (unless, as you all point out, someone goes to the extreme effort of cracking our dataset, which we hope it will be hard to do).»[3]

As it turned out, however, it was possible to identify the school in question. But the most important objection raised in the discussion about the project was the method of data collection. Zimmer

2 The description is based on Zimmer (2010).

3 Quoted in Zimmer (2010), p. 316.

criticized the absence of consent to collect information as undermining the condition for communication between the members within the network.

> While the information was indeed available to the RA, it might have been accessible only due to the fact that the RA was within the same «network» as the subject, and that a privacy setting was explicitly set with the intent to keep that data within the boundaries of that network. Instead, it was included in a dataset released to the general public.[4]

In my view, Zimmer's objection is reasonable. Facebook is a system in which participants create a framework of protected communication with selected friends by logging in and actively choosing who they want to share information with. Participants in the network express clear preferences about the limitation of access to information about themselves through their privacy settings on their profiles. Using the information for research therefore violates the conditions on which the participants' communication is based, although it is correct as the researchers pointed out that they did not do anything to expose the students to risk or discomfort.[5] The case exemplifies how data collection on the Internet can undermine the individual's interest in retaining control of the information about himself/herself, and thus trigger the requirement to obtain consent. The case also illustrates that this requirement may arise even though the research subjects are not exposed to any risk or burden. I will nonetheless assert that there is an ethically relevant distinction between research that results in a risk or burden for the participants and research that does not.

---

4 Zimmer, 2010, p. 318

5 There are open profiles on Facebook, e.g. open groups or open political profiles which, in my view, should not require consent in order to be used in research.

Reasonable expectation – of what?

In a system with a log-in function and privacy settings that limit access to personal information, it is clear in my view that consideration for the individual's interest in retaining control of information about himself/herself triggers a requirement to obtain consent. However, in contexts where the communication channel is more open, it is not as clear. In that case, some of the other factors identified by McKee and Porter may play a role: degree of vulnerability, sensitivity and degree of interaction with the research participants. I will return to this point, but first I want to discuss a particular way of formulating the requirement regarding control over information about oneself. Many have proposed that information should not be used without consent if the people being studied *do not have an expectation* that the information will be used in research. It is natural to formulate it in this way, e.g. in the assessment of research on Facebook profiles (discussed above).

Hoser and Nitschke (2009) are among those who have spoken in favour of such a formulation of the consent requirement in research on social network services.

> Thus, we could establish a simple rule: The data someone posted, e.g. in a social network site or newsgroup may be used in the context and by the audience he or she intended it for. The intended audience is, even if it is large and not personally known to the user, the «community» he or she joined. So nobody else should be allowed to use, without consent, the data generated in such a site. Researchers are probably not the audience an average user intends to reach by his or her postings and serving as a research object is normally not the purpose an average user has in mind when posting on a social network site or in a newsgroup.[6]

6 Hoser and Nitschke, 2009, page 185–186, my emphasis.

We see that the authors do not qualify which types of network services they believe should require consent, e.g. whether or not there is a log-in function. It appears they believe that if the postings were not intended for researchers, they should not be used in research. But if we formulate the criteria in this way, it will imply a consent requirement for all research, including for comments posted in the public sphere, e.g. postings in a debate forum in an online newspaper. There are two problems connected with this. One is that in some cases it is so difficult and resource intensive to obtain consent, such as from everyone who has participated in a debate on Twitter, that it is not possible in practical terms. The other problem is that it seems unreasonable to require consent in cases where people themselves seek public attention for their views, such as about political issues on Twitter. Let us look at an example.

Example 3: Research on political debate on Twitter

A Norwegian and a Swedish researcher[7] wanted to compare the political discussion on Twitter in connection with the elections held in 2012 (Sweden) and in 2011 (Norway). They used a program (TwapperKeeper) that downloads messages from Twitter related to certain #-tags, e.g. #elecl2010. They collected 100,000 messages from 9,000 individuals, which they made the object of qualitative analyses and network analyses. The question of which requirements regarding information and consent should apply in a study like this was raised in the dialogue with the Regional Ethical Review Board in Uppsala, Sweden, and the Data Protection Official for Research (NSD) in Norway. After some time, approval to implement the study in both locations without a consent requirement was received. In the assessment it was also pointed out that it would

7 Moe and Larsson (2012).

be difficult to obtain consent. The researchers' argument in this context was that the postings constituted political discussion in the public sphere, and should therefore be available for research without restriction.

> Everything that gets tweeted is public, but all of it is not necessarily for the public. Still, we would argue that the setting of our project – thematically tagged communication about an upcoming election – is public, and that the users could be expected to share that view.[8]

Note that they do not assert that all communication on Twitter should necessarily be available for research without consent: There may be communication on Twitter that should be protected. They argue for their conclusion on the basis of a concrete assessment that the channel is open, the topic is of a general political nature and the condition for discussion is that people are seeking attention for their views in a public debate.

Such a concrete assessment of how researchers should regard communication in open forums is in keeping with NESH guidelines. On the one hand, NESH says that research on open forums may be conducted without obtaining consent.

> As a general rule, researchers may freely use material from open forums without obtaining consent from those who have produced the information or those about which the information applies. For example, a researcher may freely use information obtained from the coverage an online newspaper has gathered about an issue.[9]

At the same time, NESH emphasizes in its guidelines that information that appears in open forums may also require researchers to exercise caution when disseminating research results, e.g. due to topic sensitivity or the subjects' vulnerability.

---

8 Moe and Larsson, 2011, p. 122.

9 NESH, 2003, point 4.

I argued above that it is unreasonably limiting to formulate a general requirement regarding consent if the subjects do not expect that researchers will obtain access to the information. In my view, the Twitter project discussed above is an example of a project in which the subjects do not necessarily expect that researchers will study their postings, but in which the research must nonetheless be said to be acceptable. My view is that research may be compatible with the premises for the communication situation even though the participants do not actively expect that researchers will gain access to it.

There is a logical difference between an expectation that something will not occur and the absence of an expectation that it will occur. The first implies the second, i.e. if the expression to the left of the arrow is true, the expression to the right of the arrow must also be true:

expect not-A → do not expect A,

– but the opposite does not follow.

If there is an expectation that people on the outside will not gain access, as was the case in the Facebook example, then it is a breach of this expectation to use the information in research without consent. While in the Twitter example most of the debaters do not expect that the information will be used in research, neither is it a reasonable expectation, given the context, that the information will not be used in research. Thus, in the latter instance the researchers' access to the information does not undermine the premises for communication.

The need for protection against identification

But even though researchers' access to the information does not necessarily undermine the premises for communication,

researchers will often need to give special consideration to this when disseminating their results. For instance, there are challenges related to the fact that quoting from the Internet makes it easier to search for the person being quoted. The question here is whether the further use of the research presents challenges, especially if identification is burdensome. The ethical assessments that this type of situation raises are different from those we has seen above, because the data collection in itself is burdensome or clearly infringes on the individual's interest in retaining control of information about himself/herself.

Also in cases where the researchers' access to information does not necessarily undermine the premises for communication, there may often be grounds to require consent to use the information in research, because the information is sensitive or the persons concerned are vulnerable. NESH mentions this consideration in its guidelines:

> Persons whose personal or sensitive information appears in an open forum are entitled in a research context to have such information used and disseminated in an appropriate manner. Living persons are also entitled to control whether sensitive information about themselves may be used for research purposes. The potential to trace an informant's identify is greater when using digital forums compared with other information channels […]. Researchers must anonymize sensitive information that they make use of.[10]

Regarding the third point, the assessment is more complex and the consideration for research is clearer. In this case, obtaining consent is not the only means of taking research participants into account. One alternative is to refrain from identifying the participants, but in this case a concrete assessment must be made of the specific case; it is not possible to formulate rules that can be used more or less mechanically.

10 NESH, 2003, point 6.

This also means that cases will appear in this landscape where it is not so easy to draw clear conclusions. Let me give an example.

Example 4: Research on Internet communication about mental health problems

A Swedish project, described in Halvarson and Lilliengren (2003), wanted to investigate ordinary explanations for interpersonal problems. They wanted to learn which strategies average people without formal training in psychology use when they discuss strategies for tackling life crises and personal problems. The researchers wanted to study this by monitoring open Internet forums. The participants in these forums shared their personal histories, gave advice and support to others, and related their own problems. There were many young users on the websites, and the researchers were especially concerned with how they communicated about their problems. The researchers did not obtain consent to gather this information or to quote from it.

In my view, the most difficult question in this connection is whether the researchers should quote the participants' postings, especially because it involves comments with sensitive information involving a vulnerable group. Halvarson and Lilliengren argue that it is not necessary to obtain consent to gather the information. They believe that the researchers' observation of the discussion in this open forum does not entail any risk or burden for the participants. Moreover, they point out that this is an openly available forum and that the researchers' observation and registration of the communication does not limit the participants' control over information about themselves. The question could be raised as to whether all the participants are aware of this openness to the same degree, but let us assume that the researchers are correct. They also

argue that the project is beneficial by pointing out that it is important to understand ordinary psychological explanations. Such explanations are the most important resource used by most people to tackle personal and interpersonal problems, and it is important to understand the basis for the strategies people use, e.g. for providing a basis for improving professional treatment. In addition, the researchers believe that there is no other alternative to observing natural communication, such as by setting up a discussion group and inviting people to participate in it. In this case, they believe that the recruitment would be biased and that they would not have got very many participants.

The question that remains, if they are correct that gathering information without consent is acceptable, is how the researchers should handle the information they collect when they disseminate their results. The two researchers chose to quote from the postings on the forum without giving the pseudonyms that the young people use when they participate in the discussions. The argument for this is that people often use the same pseudonym for several different Internet services, so that the names can be used in a search to find them in other places and thus help to identify them. But should the researchers have asked for consent to use the quotes they gathered? Halvarson and Lilliengren discuss this question and conclude that asking for consent could negatively affect communication in the forum:

> When studying private explanatory systems at this specific venue, obtaining informed consent is not a practical problem. All informants can be contacted via their public e-mail address and thus asked for consent to quote their postings. However, it is difficult to know how this would affect their experience and future use of the venue. If it were to be perceived as an intrusion it could have negative effects and violate later participation in discussions.[11]

11 Hallvarson and Lilliengren 2003, p. 130.

The problem is that those who receive such an inquiry might regard it as intrusion, which would decrease their interest in taking part in the forum in the future. This is obviously an important consideration. But if the researchers believe people may dislike it if they knew they were being quoted, is this not a reason to refrain from quoting their postings or to ask for their consent – especially because many of the comments are posted by young people and by people who might be in a vulnerable situation? In this case it is not easy to give a straightforward answer. It has to do in part with how great the potential is to be identified through the quotes, but it also has to do with how much the documentation is weakened by not using quotes when the results are presented, what alternatives are available for providing evidence for interpretations of the communication, and through which channels the results are disseminated. We do not have enough information to assess all of these aspects, but I would stress that there is no way to avoid a concrete assessment of all relevant values and alternatives in the situation, including the research consideration, in order to take a decision. One thing that is clear, however, is that if it is decided that consent to quote should be obtained, people should also be allowed to decide whether they want to take part in the study at all.

Example 5: Research on communication processes

The problem encountered here by Halvarson and Lilliengren is typical for many studies of communication processes: Information and questions about consent will disturb the natural interaction researchers want to study. Hudson and Bruckman (2004) have argued that in some cases like this it is acceptable to conduct research without consent, even though the researchers know that some participants in the service will dislike it. Hudson and Bruckman studied the reactions of

participants on a chat service (IRC, a moderated, synchronous service) when they were informed that they were being observed and their communication was being registered. The researchers posted information stating that a study was being conducted in four different ways in a sample of discussion threads: In some they were present with the pseudonym «chat_study», in some they only posted that registration was being carried out, in a third group they mentioned the registration and gave the email address where people could opt out, and in the fourth people received an offer to opt in. In a majority of groups the researchers were thrown out by the moderators, and in all groups they received many negative reactions. Hudson and Bruckman summarize the results of their experiment as follows:

> Based on this study, we can safely conclude that individuals in online environments such as chatrooms generally do not approve of being studied without their consent. The vehement reaction of many in our study indicates that they object to being studied. Further, when given the option to opt in or opt out of research, potential subjects still object.[12]

However, Hudson and Bruckman point out that in many groups they were not thrown out and that they do not have the chance to find out who does not want to participate in research and who is only reacting to the way the question about consent was asked. Thus they argue that it is acceptable – and the only possibility – to conduct research without consent if the IRB (Institutional Review Board)[13] rules for such research are fulfilled:

1. The research involves no more than minimal risk to the subjects.

12 Hudson and Bruckman, 2004, p. 135.

13 Independent ethical committees that oversee human subject research at each institution.

2. The waiver or alteration will not adversely affect the rights and welfare of the subjects.
3. The research could not practicably be carried out without the waiver or alteration.
4. Whenever appropriate, the subjects will be provided with additional pertinent information after participation.[14]

The key question is whether it is impossible to make the research based on consent (point 3). Hudson and Bruckman's response is that in practice it is impossible to do so because their experiment shows that in synchronous forums it is difficult to implement a recruitment process in which the researchers reach those who want to participate without disturbing the communication.

This is problematic as a general conclusion, and Bruckman and Hudson also believe that a concrete assessment must be conducted of the potential negative effects of the research. But an objection to their approach is that they do not assess alternative strategies for obtaining the consent of participants from communities on the Internet. McKee and Porter comment on Bruckman and Hudson's argument for research without consent in the following way:

> We arrive at a different conclusion: Users are not *always* hostile to researchers. However, they do not want to be studied by researchers who have not shown proper respect for the community and who have not built up some measure of respect within the community. Trust is a key element of online communication.[15]

Conclusion

I have proposed a model for ethical assessments that distinguishes between three types of situations in which the question

14 Quoted in Hudson and Brickman, 2004, p. 137.
15 McKee and Porter, 2009, p. 109.

of consent is raised when research is conducted on users of social media. Research that exposes the participants to the risk of pain or discomfort triggers a requirement to obtain consent. If the research undermines the premises for communication that the participants have given their explicit approval to, consent is also necessary for maintaining the participants' autonomy. In situations where the researchers' observation and registration of the communication do not undermine the conditions for participation, typically public debate arenas, consent is not the only way to take the research participants into account. One problem will often be how the information will be used when the research results are presented, e.g. whether quotes that may identify the participants will be used. In this assessment, consideration for the quality and value of the research should also play a role.

The properties of social media vary along many dimensions, and this is the source of uncertainty related to their ethical assessment. An important dimension is communication's degree of accessibility in the public sphere, which varies in different ways from other media. A variety of social media such as Facebook, Twitter, Instagram, Snapchat, etc. have different forms of user control, which offer different ways of limiting the audience. This helps to make it difficult to draw a clear distinction between situations where the researchers' participation undermines the premises for communication and where it does not. There may also be other considerations that affect the weight of the ethical considerations. Among these are the vulnerability of the people being studied, the sensitivity of the topic of communication, searchability of the information being presented, the degree of interactivity with those being studied, and the participants' actual competence in and understanding of how social media function.

References

Boyd, Danah (2008) *Taken out of context: American teen sociality in networked publics*. PhD thesis. University of California-Berkeley.

Halvarson, Camilla and Lilliengren, Peter (2003) Ethical and Methodological Dilemmas in Research with/on Children and Youths on the Net. I *Applied Ethics in Internet Research*, edited by May Thorseth. NTNU. 141–154.

Hoser, Bettina and Nitschke, Tanja (2010) Questions on ethics for research in the virtually connected world. *Social Networks* 32: 180–186.

Hudson, Jim and Bruckman, Amy (2004) «Go Away». Participant Objections to Being Studied and the Ethics of Chatroom Research. *The Information Society*. 20: 127–139.

McKee, Heidi A. and Porter, James E. (2009) *The Ethics of Internet Research*. Peter Lang.

Moe, Hallvard and Larsson, Anders Olof (2012) Methodological and Ethical Challenges Associated with Large-scale Analyses of Online Political Communication. *Nordicom Review*. 3 (1): 117–124.

NESH. 2009. *Forskningsetiske retningslinjer for forskning på Internett*. http://www.etikkom.no/Forskningsetikk/Etiske-retningslinjer/Samfunnsvitenskap-jus-og-humaniora/Internett-forsking/. Downloaded 5 July 2013.

Zimmer, Michael (2010) "But the data is already public": on the ethics of research in Facebook. *Ethics and Information Technology*. 12: 313–325.

Possibilities and limitations of Internet research: A legal framework

Katrine Utaaker Segadal
Norwegian Social Science Data Services (NSD)
katrine.segadal@nsd.uib.no

As the data protection official for research for some 150 Norwegian research and educational institutions, NSD has noticed an increase in research conducted on data harvested from the Internet in recent years. Today, the Internet is an important arena for self-expression. Our social and political life is increasingly happening online. This will have a major impact on how we understand the society in which we live and the opportunities for future generations to reconstruct the history of the 21st century.

Thus, data generated by the growth in electronic communications, use of Internet and web-based services and the emergence of a digital economy are increasingly valuable resources for researchers across many disciplines. At the same time there is a great need for knowledge and awareness of both legal requirements and ethical challenges related to the use of these new data sources, and for an understanding of the data's quality and scientific value.

In addition to the increased volume of this type of research, we have also seen a shift in focus. At first, the Internet and social media were studied mainly as a tool. The studies often concentrated on how the Internet worked as an instrument in e.g. education, health services or online dating. The methodological approach was usually interviews or surveys based on informed consent from the research subjects.

Today, the trend is to study the Internet as an arena for expressing or negotiating identity, often through projects of a sensitive character (e.g. political opinion, religious beliefs, health). Data are usually collected from social media such as blogs, social networking sites or virtual game worlds. These sources are publicly available, and often research is conducted without informed consent from the persons being studied.

This development raises questions such as: Which rules and regulations apply to research on personal data collected from the Internet? In which cases is it legal and ethical to conduct research on such data without the consent of the data subjects? When is it necessary to inform the data subjects of their involvement in a research project and when should this information be accompanied by an opportunity to refuse to be the object of research? These issues will be discussed in further detail in the following.

New European legislation in the making

The use of new types of data, such as those collected online and so-called Big Data, rank high on the international agenda. The OECD Global Science Forum points out the challenges related to the large amounts of digital data that are being generated from new sources such as the Internet although these new forms of personal data can provide important insights,

> the use of those data as research resources may pose risks to individuals' privacy, particularly in case of inadvertent disclosure of

> the identities of the individuals concerned. There is a need for greater transparency in the research use of new forms of data, maximizing the gains in knowledge derived from such data while minimizing the risks to individuals' privacy, seeking to retain public confidence in scientific research which makes use of new forms of data.[16]

To address this challenge, the forum recommends that research funding agencies and data protection authorities collaborate to develop an international framework that protects individuals' privacy and at the same time promotes research.

The European Commission has proposed a comprehensive reform of the EU's 1995 data protection rules,[17] and we might see the results of this in the relatively near future if and when the new General Data Protection Regulation is implemented in Norwegian law. EU Justice Commissioner Viviane Reding said on the occasion of the legislative proposal:

> 17 years ago less than 1 % of Europeans used the Internet. Today, vast amounts of personal data are transferred and exchanged, across continents and around the globe in fractions of seconds. The protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data. My proposals will help build trust in online services because people will be better informed about their rights and in more control of their information[18].

We will not go further into this, but just briefly mention that the new digital media, and the Internet as an increasingly significant

16 OECD Global Science Forum (2013): «New Data for Understanding the Human Condition: International Perspectives», page 2.

17 http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

18 European Commission – IP/12/46 25/01/2012 – Press release: «Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses» http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

data source, are important reasons why the EU is currently upgrading the data protection regulation from directive to law. A regulation is a binding legislative act and must be applied in its entirety across the EU. **Directives** lay down certain results that must be achieved by all EU countries, but the individual Member State is free to decide how to transpose directives into national laws.

The demand for harmonization of rules and practices is high, particularly related to the use of data generated by or in relation to global communication networks such as the Internet. This type of network weakens the significance of national borders and the impact of national policies and legislation on the protection of personal data.

NSD's general impression of the Commission's initial proposal was that it would not lead to any dramatic changes for Norwegian research. The reason is primarily that Norwegian data protection legislation and the way this legislation is practised in relation to research are stringent, and that we have a high degree of protection of personal data in Norway. However, some of the recently proposed amendments to the Commission's proposal made by the European Parliament may have negative consequences for parts of the research sector if being transposed into EU legislation. There is a clear tendency in this proposal towards strengthening the right to personal privacy and control of own personal data at the expense of researchers access to such data.

The current Norwegian legal framework

In Norway there are primarily three laws (i.e. the Personal Data Act, the Personal Health Data Filing System Act, and the Health Research Act) that regulate the use of personal data for research purposes. In cases of collecting research data from the Internet, it is mainly the Personal Data Act that applies, so our focus will be on this.

Although the regulations are not always crystal clear, they provide important guidelines on how data initially produced for other purposes can be used for research purposes. The regulations may set limitations on usage, but they also provide many opportunities for valuable research.

The Personal Data Act is technology-neutral, although it is not necessarily adapted and updated with regard to technological development. The law applies to the processing of personal data, irrespective of source. It is applicable regardless of whether the data are self-reported, collected from a confidential source or gathered from a public registry. This implies that a research project is subject to notification to the Data Inspectorate or Data Protection Official when personal data are processed by electronic means, even if the information is gathered from a publicly available source on the Internet.

Data protection principles online

The purpose of the Personal Data Act is to protect the individual's privacy from being violated through the processing of personal data.[19] Key principles of data protection are the need to protect personal integrity and private life, to ensure individuals' control of their own personal data and to guarantee that personal data are of adequate quality. These important principles are the basis for the interpretation of other provisions in the Personal Data Act, and place restrictions on research on information obtained from the Internet. They are closely related to essential principles of research ethics such as the demand to respect human dignity, integrity, freedom and right to participate, and the obligation to prevent harm and suffering.[20]

19 Act of 14 April 2000 No. 31 relating to the processing of personal data, section one.

20 The National Committee for Research Ethics in the Social Sciences and the Humanities (NESH) (2010): *Guidelines for research ethics in the social sciences, law and the humanities*, chapter B.

These data protection principles are applicable irrespective of methods for data collection and data sources involved in the research. Consequently, they also apply to data collection online. However, handling these fundamental data protection principles in this context presents the researcher with certain challenges. Should one expect those who express themselves online to understand that their personal data may be used for purposes other than those originally intended, such as research? Have they given up control of their personal data when publishing on the Internet? And how does the availability of the data affect the researchers' duty to protect the privacy and personal integrity of the persons being studied? As a researcher it might be helpful to consider the following when trying to figure out these issues.

First of all, from what type of medium are the data obtained? Data collected from a public forum for debate will probably require fewer safeguards than a Facebook page with access restrictions. Second, does the data have the character of a public statement or is it reasonable to presume that the information is meant to be of a private and personal kind? And further, should the information be safeguarded considering the data subject's best interests, irrespective of medium or the author's assumptions? Sensitive data (e.g. information related to health) might require a high level of protection, even though it is published as part of a public statement at an open webpage. One might claim that the researcher has a special responsibility to protect sensitive personal data although the subject has disclosed it voluntarily, bearing in mind that the person might not view the full consequences of publishing the information online.

A fourth important factor is whether the data subject is a child or an adult. Information concerning children is subject to strict regulations. In 2012 a new provision of the Personal Data Act

was implemented. The Act states that «[p]ersonal data relating to children shall not be processed in a manner that is indefensible in respect of the best interests of the child».[21] In the draft bill this provision is partly justified by the challenges associated with children's use of new technology. The ministry especially points out problems related to adults' attitudes towards publishing images of and information about minors. The most serious violations of children's privacy are increasingly committed by adults. This provision could also apply to a website's use of material voluntarily published by children themselves, if this use is indefensible.[22] In this case further use by researchers might be illegal and unethical.

Furthermore, in relation to this, one should consider whether the information is published by the data subject itself or by a third party. If there already has been a breach of data protection principles, which may be the case when it comes to information published by another person than the data subject, researchers should be particularly careful.

Research without consent

As a default rule, personal data cannot legally be used for purposes other than the original one, unless the data subject consents.[23] And it is fair to assume that those who have published data on the Internet have not done so with the purpose of being the object of research. However, the Personal Data Act includes a number of exemptions from the general rule for research.

21 Act of 14 April 2000 No. 31 relating to the processing of personal data, section eleven, third paragraph.

22 Prop. 47 L (2011–2012) Proposisjon til Stortinget (forslag til lovvedtak) Endringer i personopplysningsloven, Chapter five.

23 Act of 14 April 2000 No. 31 relating to the processing of personal data, section eleven, first paragraph, litra c.

An important provision in this respect is that

> subsequent processing of personal data for historical, statistical or scientific purposes is not deemed to be incompatible with the original purposes of the collection of the data, cf. first paragraph, litra c, if the public interest in the processing being carried out clearly exceeds the disadvantages this may entail for natural persons.[24]

Thus, research activities are, per definition, not considered incompatible with the original purpose. Science is afforded a special position in the current legal framework, and this provision might be seen as a fundamental principle guaranteeing further use of data for research purposes regardless of the original reason for their production. This leaves open the possibility to conduct research on information obtained online without consent.

Having said that, as a general rule personal data may only be processed when the data subject has freely given an informed consent.[25] When designing a research project, the starting point should always be to consider whether consent should and could be obtained prior to the collection of data.

However, another provision offers a direct exemption from the main rule. Even sensitive personal data may be processed if this «is necessary for historical, statistical or scientific purposes, and the public interest in such processing being carried out clearly exceeds the disadvantages it might entail for the natural person».[26]

Firstly, this entails that the planned processing of personal data must be required to answer relevant research questions. The

24 Act of 14 April 2000 No. 31 relating to the processing of personal data, section eleven, second paragraph.

25 Act of 14 April 2000 No. 31 relating to the processing of personal data, section eight, first paragraph and section nine, litra a.

26 Act of 14 April 2000 No. 31 relating to the processing of personal data, section nine, litra h.

researcher has to make it probable that the planned harvesting of data from the Internet is absolutely necessary to achieve the purpose of the study.

Secondly, if the necessity requirement is met, the law requires a balancing of interests between the project's societal value and any possible inconvenience for the individuals who are subject to research. It is crucial that the research will benefit society in some way or at least be an advantage for the group that is being researched. When assessing the probable disadvantages for the data subject, relevant factors are the degree of sensitivity, the author's presumed purpose of publishing (e.g. private or freedom of expression), the source (e.g. forum with restricted access or publicly available), who the data subject is (e.g. child, vulnerable/disadvantaged individual, adult) and the degree to which the data subject is identifiable.

Another important aspect to keep in mind in deciding for or against the processing of personal data for research purposes without consent is whether or not it will be possible to publish the results anonymously. This may be a challenge if one wishes to publish direct quotes, as these will be searchable on the Internet. It is also important to note that pseudonyms or nicknames may be identifiable because they may be used in various contexts online and hence function as a digital identity.

Moreover, an important factor is whether the data subject is informed of the research project. Having information and the opportunity to object to being included in the research will limit the disadvantages because the individual will then be able to exercise control over his or her own personal data. This may be a weighty argument for exempting a research project from the consent requirement. However, the right to object is not in itself considered a valid consent under the Personal Data Act. A valid consent must be a freely given, active and specific declaration by

the data subject to the effect that he or she agrees to the processing of personal data relating to him or her.[27]

If a research project includes the processing of highly sensitive data (e.g. from blogs about personal experiences with eating disorders, self-harm or the like), and the information being processed is detailed enough to make the bloggers identifiable (a factor one generally must take into account), it may be difficult to exempt from the requirement for consent. This holds particularly if publishing direct quotes is deemed necessary by the researcher, so that it will be hard to guarantee anonymity in the publication. If the authors are minors, the threshold for not obtaining consent should be even higher. Adolescents over the age of sixteen will often be considered mature enough to give an independent consent in such cases. However, when obtaining consent online, it might be a challenge to be certain of the actual age of the person granting consent.

In the case of research on utterances from Twitter, which involves thousands of people, that focus on e.g. elections (which in the legal sense may be sensitive information about political views), there will clearly be legitimate reasons not to obtain consent from the data subjects considering the public character of both the source and content of the data.

In between these two rather clear-cut examples lies a range of grey areas which require concrete assessments in each case. My main message is that it certainly can be legal to conduct research on personal information obtained from the Internet without consent, as long as the researcher can justify the necessity and the benefits for the public clearly outweigh the disadvantages for the individual. The violation of personal privacy is often minimal when data is harvested on the Internet for research purposes. However, research

27 Act of 14 April 2000 No. 31 relating to the processing of personal data, section two, number seven.

on social media with restricted access differs somewhat from most other contexts in this respect. It is plausible that individuals who publish information about themselves under such circumstances might think that they are acting on a «private» arena, and that their purpose is to interact with a closed group of people. This indicates that the threshold should be slightly higher when considering not obtaining consent in such cases.

Obligation to provide information

The general rule is that the research subjects should be informed about the research. This is the case even if the exception clause from the requirement for consent applies. The basis for this rule is the fundamental right to exercise control over one's own personal data, and the assumption that the data subject should have the right to object to the intended processing of her personal data. However, a relevant exemption provision allows for research to be conducted without informing the data subjects: «The data subject is not entitled to notification […] if […] notification is impossible or disproportionately difficult».[28]

If it is not feasible to get in touch with the affected individuals because it is not possible to obtain contact information or to communicate through the website, there is of course no way to provide those individuals with information.

Relevant factors in the assessment of whether it is disproportionately difficult to provide information are, on the one hand, the number of data subjects and the effort, either in terms of time or money, that providing information would entail. However, technological developments are and will most likely make it increasingly easier to distribute information to thousands of individuals at the

28 Act of 14 April 2000 No. 31 relating to the processing of personal data, section 20, second paragraph, litra b.

same time at no extra cost. The violation of personal privacy is not automatically less because the data subjects are numerous.

On the other hand, one should consider what use the data subject will have of being informed of the research project. Is it likely that the research subjects would wish to object if they had the opportunity to do so? If that is a reasonable assumption, information should be provided. Another important question is to what extent the research subjects will benefit from being able to refuse to be part of the research project. This will depend on the type of data being processed and how sensitive the information is. If what is at stake is very sensitive information, data protection principles indicate that information should be provided. This holds independently of whether the data subject initially has made the information publicly available.

Legally, the obligation to provide information is met only if the researcher gives individual information in such a way that the information is certain to reach the intended receiver. But in some cases, it may be appropriate to provide public information instead. This may be done through collective information published on the website from which the data is collected. It is not guaranteed that this information will reach everyone in the same way as when it is communicated directly by mail, email or other channels, but public information is nevertheless a measure that, to a certain extent, can justify exemptions from the requirement of individual information.

Conclusion

The Personal Data Act is applicable irrespective of the data source. The regulations do not distinguish between data harvested from the Internet and other sources (such as administrative registers). However, the legal framework leaves open a range of possibilities

for conducting research on information obtained online. It might be challenging, though, to apply the rules in this context.

The main rule is that the processing of personal information should be based on informed consent. But a number of exemptions make it possible to conduct research on personal information obtained from the Internet without consent, as long as the researcher can justify the necessity, and the benefits for the public clearly outweigh the disadvantages for the individual. The violation of personal privacy might often be limited when data is harvested on the Internet for research purposes.

References

European Commission – IP/12/46 (25/01/2012) – Press release: «Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses» http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en (Accessed 13 February, 2014).

Justis- og politidepartementet (2011): Prop. 47 L (2011–2012) Proposisjon til Stortinget (forslag til lovvedtak) Endringer i personopplysningsloven.

Ministry of Justice and Public Security: Personal Data Act, Act of 14 April 2000 No. 31 relating to the processing of personal data.

The National Committee for Research Ethics in the Social Sciences and the Humanities (2010): «Guidelines for research ethics in the social sciences, law and the humanities».

OECD Global Science Forum (2013): «New Data for Understanding the Human Condition: International Perspectives».

New selves, new research ethics?

Charles Ess

Department of Media and Communication,
University of Oslo

c.m.ess@media.uio.no

Introduction

The first set of ethical guidelines explicitly devoted to Internet research appeared only in 2002 (Ess et al. 2002). Norway published its own set of Internet Research Ethics guidelines soon thereafter – and remains the only nation to have done so (NESH 2003). And IRE (Internet Research Ethics) continues to develop and mature. As but one example, the first set of AoIR guidelines has now been supplemented with a second (Markham and Buchanan 2012). It is certain that IRE will continue to develop and expand – first of all, as pushed by constant changes in the technologies involved. Here, however, I focus on a still more fundamental transformation – namely, profound changes in our sense of selfhood and identity.

Perhaps the most foundational element in ethical reflection is our set of assumptions regarding the human being as a *moral agent* – and thereby, what sorts of *responsibility* s/he may be legitimately considered to hold. I begin by showing that until very recently – certainly past the publication of the first AoIR guidelines – our primary ethical theories and approaches rested on the assumption that human identity is primarily singular and *individual*: and

thereby, moral *agency* and *responsibility* were tied directly – and, most often, exclusively – to single individuals. But for several decades now, our conceptions of human selfhood and identity have begun to shift towards various *relational* conceptions – conceptions that stress a sense of identity as inextricably interwoven with various relationships (familial, social, natural, and so on) that define us as *relational* selves. These foundational shifts are accompanied by changing conceptions regarding morality and responsibility: as we will see, there are emerging efforts to understand at both theoretical and practical levels what «distributed responsibility» and «distributed morality» might look like. That is: as our ethical agency is thereby shared and distributed among the network of relationships that define us as relational selves, so our ethical responsibilities are likewise distributed and shared. Hence we are witnessing the development – and in some ways, a rediscovery – of forms of distributed morality more appropriate to such relational selves.

These shifts thus require a transformational rethinking of our ethical frameworks and approaches – including within Internet Research Ethics. Indeed, IRE is a primary domain within which to explore and develop these transformations: relational selfhood is most apparent as it is performed or enacted precisely through the communicative networks at the focus of IRE. At the same time, Norway may play a distinctive role in these transformations. Norwegian research ethics has already recognized in at least one important way that we are indeed relational selves: it has enjoined upon researchers the ethical duty of protecting the privacy and confidentiality of not only the *individual* research subject, but also his or her close circle of personal relationships (NESH 2006, 17). In this way, Norwegian research ethics provides a critical first example of how, I will argue, IRE will develop further, as both researchers and their relevant oversight institutions (such as institutional review boards in the U.S.) begin to take on board these foundational shifts in selfhood.

In the following, I will highlight how modern conceptions of the individual self lead to distinctively modern expectations regarding *individual* privacy as a positive good and right. Protecting such privacy, moreover, has been a core requirement for Internet researchers. But this means that our changing conceptions of selfhood entail shifting – and in some ways, more complex – conceptions of privacy. In particular, the recent work of Helen Nissenbaum, which defines privacy in terms of «contextual integrity» (2010, 107 ff.), appears to mesh well with more relational conceptions of selfhood. Lastly, in order to explore these matters in applied ways, I will describe three recent research projects, each of which involves participants' installing apps on their smartphones that record and transmit enormous amounts of information, much of which appears to implicate what we do in our most intimate spaces. We will see that extant guidelines and legal protections of rights seem sufficient for establishing the ethical obligations of the researchers involved. The failure of a third project, however, points to the need for new frameworks and guidelines for protecting the new forms of privacy attending upon more relational selves.

Initial (high modern) ethical frameworks for decision-making in (Internet) research ethics

Internet Research Ethics began to expand rapidly in the early 2000s (Buchanan and Ess 2008). This expansion followed a handful of scattered U.S. governmental reports, a landmark 1996 special issue of the journal *The Information Society* devoted to IRE, and a watershed 1999 workshop on IRE funded by the National Science Foundation and the American Association for the Advancement of Science. The 2002 AoIR guidelines for Internet research were the first such set of guidelines issued by

a professional organization; these were followed by the NESH 2003 guidelines – again, the only national guidelines focusing specifically on Internet research. In the next few years, other professional organizations in the U.S. and the U.K. issued Internet-specific guidelines; at the same time, a small explosion of articles and, indeed, whole anthologies devoted to IRE appeared (see Buchanan and Ess 2008: 274 for details).

From an ethical perspective, these diverse documents drew from one of three primary ethical theories: utilitarianism, deontology, and feminist ethics (Stahl 2004; Buchanan and Ess 2008: 274–277). As a brief reminder, *utilitarian* approaches take what we can think of as a kind of ethical cost-benefit analysis: given a set of possible choices before us, what are the (potential) benefits of a given choice (or rule of choice in what is called rule utilitarianism) vis-à-vis the (possible) harms of that choice? Benefits and harms here are initially defined in terms of pleasures, whether simply physical and/or intellectual pleasures. Hence the goal of such ethics is to pursue those choices that maximize pleasure. At the same time, however, utilitarianism argues that the ethically justified choice is not simply the one that would maximize *individual* pleasure: rather, utilitarianism famously aims at «the greatest good for the greatest number.» Utilitarianism first developed in the U.K., beginning with Jeremy Bentham (1748–1832) and perhaps most prominently with John Stuart Mill (1806–1873). Perhaps not accidentally, utilitarian approaches appear to predominate in the English-speaking world, including the U.S. and the U.K. (Buchanan and Ess 2008: 276).

By contrast, *deontology* emphasizes the basic rights of autonomous individuals – including rights to life, liberty, pursuit of property, and, as we will explore more fully below, *privacy*, etc. – as near absolute. This means that these rights are to be protected (more or less) no matter what benefits might otherwise accrue

from reducing or eliminating such rights. That is (to take a simple example): a primary critique of utilitarian approaches is that they allow for the sacrifice of the few for the sake of the many. In some cases, we may agree that this is an ethically legitimate choice, e.g. as when we ask police, firefighters, or soldiers to risk their lives in ways that might bring them great pain, or even loss of life – but at the very great benefit for the rest of us of preventing great harm and saving (potentially many) lives. But a similar utilitarian cost-benefit analysis could likewise demonstrate that, whatever the negative costs of enslavement might be experienced by slaves in a possible slave-based society, these costs are dramatically outweighed by the accordingly greater pleasures of the slaveholders. If we immediately reject such a proposal, despite its sound utilitarian calculus, this is most likely due to the fact that we are deontologists who hold that all human beings have basic rights, beginning with rights of autonomy and self-determination: these rights must be upheld, no matter the possible benefits of diluting or eliminating them.

Deontological ethics are primarily affiliated with the work of Immanuel Kant (1724–1804). Kantian deontologies appear to enjoy greater currency in the Germanic-language countries, including Denmark, Norway, and Sweden – first of all, as manifest in the profoundly influential conceptions of the public sphere and democratic processes as rooted in rights of self-determination and autonomy as developed by Jürgen Habermas (Buchanan and Ess 2008: 275).

Finally, feminist ethics is occasionally invoked by researchers, especially in connection with participant-observation methodologies (e.g. Hall, Frederick & Johns 2004). As we will see below, feminist ethics contributes to recent shifts away from more sharply individual conceptions. For that, feminist ethics has remained relatively marginal in IRE.

Shared assumptions: (high modern) Individual agency, privacy, and IRE

As diverse as utilitarianism and deontology are, they nonetheless share a more foundational set of assumptions – namely, the (high modern)[29] understanding of human beings as primarily autonomous *individuals*. This is apparent first of all in the English-speaking traditions of utilitarianism, as these build on a sense of selfhood and identity developed especially by the philosopher John Locke (1632–1704). Locke argues for what Charles Taylor characterizes as a «punctual self» – one that is radically reflexive and rational. Such an atomistic conception of selfhood thereby enjoys a (high modern) sense of radical independence, «free from established custom and locally dominant authority» (Taylor 1989: 167). This radical freedom thereby entails a radical responsibility – for the cultivation of our own selfhood, first of all, and thereby, our own sense of what aims and goals we choose to pursue from the standpoint of such radical freedom. *Contra* more relational senses of selfhood as interwoven with and thus bound to the various authorities and institutions that defined community, society, and political life in pre-modern eras – these high modern selves are «creatures of ultimately *contingent* connections» (Taylor 1989: 170). That is, rather than accepting community traditions, practices, and institutions (most obviously, political and religious institutions) as defining the meaning and goods of our lives, such high modern individuals *determine for themselves* what connections with other individuals and institutions they will take up. These connections, finally, «are determined purely instrumentally, by what will bring the best results, pleasure, or happiness»

29 The distinction between «high modern» and «late modern» is taken from Anthony Giddens (1991: 70).

(Taylor 1989: 171). «Pleasure» and «happiness» here point in the direction of utilitarianism.

The emphasis on individual selfhood is equally apparent in Kantian deontology as anchored in core notions of ethical *autonomy*. «Autonomy» is a term developed from Greek, meaning literally self-rule (*auto-nomos*). In Kant's procedural ethics, this autonomy is expressed precisely in the strictly rational analyses defined by his categorical imperative: «So act that the maxim of your will could always hold at the same time as a principle establishing universal law» (Kant [1788] 1956: 31). This decision-making process seeks to determine whether a given act is ethically legitimate by asking the question whether or not we can endorse the general principle that would result from rendering our choice into a universal law. On the one hand, this decision-making process shows ethics to be an intrinsically relational affair in at least two ways. One, the sort of reason (*Vernunft*) at work here is presumed to be a faculty shared among and largely similar between all human beings (indeed, all rational beings). Two, the question of generalization is thus a question of how far we can will our acts to be the principles of others' acts as well. At the same time, however, this decision-making process rests squarely on the individual and the individual alone.

And so in both traditions, the moral agent is presumed to be a solitary individual. Confronted with a specific ethical choice, such an agent is envisioned as considering her possibilities and options as a solitary being, apart from the voices, influences, and perhaps coercion of others. Moreover, whether making her choice through a more deontological or more utilitarian approach, the moral agent is thereby the entity who bears the sole and exclusive *responsibility* for that choice.

(High modern) notions of selfhood/ identity: Privacy as a positive good

This strongly individual conception of human beings is thus the subject that both justifies and demands democratic-liberal states – and with these, basic *rights*, beginning (in the U.S., but based on Locke) with rights to life, liberty, and pursuit of property. More gradually, *privacy* emerged as a primary right to be enjoyed and protected by such individuals. In the case of the United States, this required a period of nearly a century, from the amendments to the U.S. Constitution (1789) to the first explicit defense of *privacy* as a right – specifically, the right to be left alone and free from intrusion (Warren & Brandeis, 1890). As Bernhard Debatin points out, the concept is rooted in Fourth Amendment protections against «unreasonable search and seizure» of private property, among others (2011: 49). Subsequently, both the meaning of «privacy» and thereby its justifications have developed in several directions – and in ways that vary importantly from culture to culture. Broadly, privacy can be defined as an «expressive privacy,» one that «protects a realm for expressing one's self-identity or personhood through speech or activity» – without fear of repercussion from others (DeCew 1986, cited in Meeler 2008, 153). Such privacy is requisite first of all for one's own *self*: «expressive privacy sustains *an arena within which one can freely select behavior* that *maximizes one's expression of self*» (Meeler 2008, 157; emphasis added). Such privacy, as a zone of exclusion that prohibits others from entering, is required further to serve *decisional privacy*: that is, private space is a necessary condition for ethical reflection and decision-making of either the utilitarian or deontological sort. Broadly, such a space is required if we are to deliberate, reflect, critique alternatives, and thereby *freely* choose or judge what is to be one's own conception of the good life. This includes deliberating on and then determining one's political, religious, career, and

other personal choices and commitments (in Kantian language, one's *ends*) and thus the appropriate and necessary *means* for achieving those ends. As U.S. philosopher Deborah Johnson emphasizes, such privacy is needed for the self to develop as an autonomy thereby able to participate meaningfully in debate and other democratic practices (Johnson 2001: for additional national examples, see Ess 2013a: 44–47, 62–68).

We can also note that U.S. conceptions of privacy and privacy rights are squarely *individual*. By contrast, discussions of privacy in Denmark and Norway, for example, use the terms *privatlivet* («private life») and *intimsfære* («intimate sphere»). Very briefly, private life is considered to include the close relationships that make up one's «intimate sphere.» To highlight the importance of protecting *privatlivet* thus entails protecting not simply the privacy of the individual, but also the privacy of those whose close relationships constitute one's *intimsfære*.

Finally, we need to be clear how such a conception of privacy – specifically, of *individual* privacy as a *positive* good – thereby basically reverses earlier understandings of privacy. These earlier understandings – in both the pre-modern West and in multiple non-Western societies – turned first of all on a very different conception of selfhood and identity. Most briefly, throughout most of human history, and in cultures distributed globally (e.g. as influenced by Buddhist and Confucian traditions, as well as in multiple indigenous societies) – the prevailing emphasis in foundational conceptions of identity is precisely on the *relationships* that define who one is. These relationships are first of all familial – i.e. defined by your parents and grandparents (and their ancestors in turn), your siblings, your aunts and uncles, and, if you have them, your spouse and children. In this view of the self, notions of privacy as a positive good are only *relational* notions – e.g. of familial privacy vis-à-vis the larger village in traditional Thai society (Kitiyidasai 2005). Consequently, should an individual want to be alone or

away from the relationships that define him or her, the motives for doing so can only be suspect. So it is, for example, that until 1985 the only word for privacy in Chinese – *yinsi* – was defined as something shameful, hidden, or bad (Lü 2005).

Individual privacy as definitive for «traditional» Internet Research Ethics

With this as a background, we can now see how high modern, strongly individual notions of privacy and privacy rights have been foundational to Internet Research Ethics. In the U.S., to begin with, IRE is rooted in human subjects protections that grew up after both «internal» scandals such as the Tuskegee Institute syphilis study and the horrors of Japanese and Nazi «experimentation» with prisoners during WWII. Protecting the privacy of individuals is an explicit requirement – along with other protections of anonymity, confidentiality, and identity that likewise serve to protect individual privacy (see Buchanan and Ess 2008: 277–281).

Again, how we are to implement such protections varies – first of all, depending on whether we take a more utilitarian or more deontological approach. For example, IRE in the U.S. context characteristically discusses the need to *balance* individual rights (including rights to privacy) with possible benefits to the larger society (and, perhaps, the individual subject). The usual language emphasizes a need to minimize the risk of possible harm – reflecting the utilitarian view that the greater good for the many can justify at least marginal costs to the few (especially if, like firefighters and police, they freely agree to undertake the risks involved). By contrast, the NESH guidelines (2003, 2006) emphasize that the rights of human subjects must never be compromised, irrespective of the potential benefits – an emphasis consistent with the stronger reliance in northern Europe on more deontological approaches (Buchanan and Ess 2008: 276).

We can also see some difference between U.S. and Norwegian approaches in terms of *who* is to be protected as a research subject. In general, U.S. regulations focus squarely – as we would expect – on the research subject as an *individual*. By contrast, the NESH guidelines (2003, 2006) further include the explicit obligation «to respect individuals' privacy [*privatlivet*] and close relationships [*nære relasjoner*] (NESH 2006 B.13, p. 17). To be sure, there is some concern noted in the relevant U.S. codes for the need to protect «third party information» that is gathered from a primary subject, e.g. about his or her friends or close relations (Protection of Third Party Information in Research 2001). And by 2011 there is recognition that human subjects protections may be required for such secondary or tertiary subjects (UCLA OHRRP 2011). Nonetheless, Annette Markham observes that the need to protect the privacy of not only the primary subject but also his or her close relationships is only «vaguely addressed» in the U.S. codes. By contrast, «the NESH guidelines are the most specific, and I think even more importantly, articulated in a way that seems to make it a critical part of the central goal of privacy protections.»[30] This inclusion would seem to closely correlate with the greater emphasis on relational dimensions of selfhood in Norwegian privacy discussions. In these ways, the NESH guidelines appear to assume a sense of selfhood or identity that is *both* singular *and* relational. That is, singular or individual identity is apparent in the need to protect individual rights to privacy (*privatlivet*) – as the importance of relational identity is apparent in the need to respect the close relationships that constitute one's *privatlivet* in good measure. While heading in the direction, we might say, of more traditional or classical conceptions of selfhood as (fully) relational, the NESH guidelines clearly retain a strong – indeed, fully deontological – emphasis on the rights of the individual.

30 Annette Markham, personal communication. I would also like to express my deep gratitude to Annette Markham and Elizabeth Buchanan for their expert help and invaluable references on this point.

Insofar as this is true, as we are about to see, the NESH guidelines thus stand ahead of the curve of change and development that seems required in IRE as our conceptions of selfhood in Western societies are changing more broadly.

(Late modern) shifts in selfhood, responsibility and privacy

To be sure, strong notions of individual privacy became ever more fully encoded and protected in various ways in Western societies throughout the 20th century. In light of the rise of networked communications in the latter half of the 20th century, perhaps most important among these were developing notions of *informational privacy*, our having the ability to control information about us that we consider to be personal (Tavani 2013: 136). Perhaps somewhat paradoxically, however, at the same time conceptions of selfhood in Western societies began to shift away from strongly individual conceptions towards more explicitly relational ones (3.1). These shifts, as we will further see, correlate with changing conceptions of privacy and expectations of privacy protections (3.2) – and, finally, with the development of new philosophical theories of privacy as well (3.3).

Changing conceptions of selfhood and responsibility

Within philosophy, as we have seen, conceptions of selfhood even at the time of Kant and Hegel were not *exclusively* individual, but also included the social or the relational (cf. Hongladarom 2007). Building on Kant, in particular, Habermas's theory of communicative action (1981) highlights a conception of communicative reason as relational (McCarthy 1978: 47). Identity is thus a social

identity, one inextricably interwoven with and thus shaped through our engagements with others (cf. Ess 2013b: 217).

Twentieth century philosophy included several other emerging movements that likewise emphasized the social or relational dimensions of selfhood, beginning with phenomenology. So Maurice Natanson reversed Descartes' famous dictum, *cogito ergo sum* (I think, there I am) with the statement «We are. Therefore I am» (1970: 47). Inspired in part by ecological ethics (i.e. an ethics that emphasizes precisely our inextricable interdependence upon one another), feminist theorists and researchers, beginning with Carol Gilligan, found that women as a group tend to emphasize not simply individual interests, choices, etc., but also those represented within the «web of relationships» that formed the context for specific ethical decisions (1982). More recently, *virtue ethics* has experienced a renaissance – most remarkably vis-à-vis contemporary networked communication technologies such as social networking sites (SNSs). Virtue ethics, in both ancient and contemporary cultures and settings, addresses precisely the situation of more relational selves, as it stresses our learning how to establish and foster community harmony as a key component of both individual and community contentment or happiness (*eudaimonia*) (e.g. Hursthouse 2012; cf. Vallor 2009, 2011, 2012).

Similar shifts can be seen in the literatures of psychology and social science. So Georg Simmel describes the self as a «sociable self» (1955, 1967). For his part, George Herbert Mead inaugurates «the social theory of consciousness» that reiterates the sense we have seen in 20th century philosophical theories that individual identity first emerges out of a shared, social identity ([1934] 1967: 171). As a last example, Erving Goffman describes the self as defined by its roles and relationships that are then performed and managed in different ways (1959).

These social and psychological accounts are of particular import as they have become prevailing theories for studying our engagements with one another in the online and mediated contexts

facilitated by Internet communication. This relational – but still also individual – self is further apparent in more contemporary work in IS, beginning with the widely used conception of the self as a «networked individual.» Michelle Willson summarizes this conception as stressing how «the individual experiences her/himself as largely in control of her/his sociability through the possibilities of the [network] technology,» a view that highlights such individuals as «compartmentalized or individuated persons who approach and engage in constitutive social practices in ways chosen by themselves» (2010: 498). As Willson goes on to point out, this view is criticized for overstating the possible agency – if not narcissism – of such an individual, precisely at the expense of our social and the relational dimensions (2010: 499 f.). By the same token, still more overtly relational conceptions of selfhood have also come to the foreground (e.g. Gergen 2009). This is to say: much of contemporary Internet research presumes a self that is both individual *and* relational – while our prevailing codes and guidelines for Internet research ethics remain grounded in an exclusively individual conception of selfhood, as we have seen.

These shifts, finally, are recognized within philosophy to require correlative changes in our conceptions of ethical responsibility. As a first example, contemporary feminists are developing notions of «relational autonomy» that build on these various recognitions that our sense of selfhood and agency is interwoven through and defined by our relationships with others; at the same time, the notion of relational autonomy retains earlier (high modern) understandings of moral agency and responsibility as connected with strongly individual notions of selfhood (Mackenzie 2008). Two philosophers who attend especially to computation, networked computing and the networked communications facilitated by the Internet have further contributed to these emerging notions. Judith Simon details how such networks embed us in a «distributed epistemic

responsibility» (2013), and Luciano Floridi provides both a theoretical account for and practical examples of what he calls distributed morality and distributed (ethical) responsibility (2012). These notions of distributed epistemic and ethical responsibility are clearly coherent with the more relational emphases of selfhood and identity afforded by online and mediated environments.

Changing privacy practices and expectations of privacy protections

These shifts in our philosophical, sociological, and psychological conceptions of selfhood further appear to correlate with observed *practices* and «performances» of privacy in online and mediated environments. Broadly, it seems clear that especially in the last two decades, we have witnessed a rather dramatic shift from strongly individual notions of privacy to various forms of «group privacy» – i.e. precisely the sense of wanting to protect information shared within a close circle of friends or relations (an *intimsfære*).

As a first example: especially with the emergence of social networking sites (SNSs) in the early part of the 21st century, it is a commonplace for parents to complain and worry about information their adolescent children post in such settings. Simply put, from the parents' perspective, their children are revealing far too much *private* information about themselves. To be sure, these worries are not always misplaced. Well-known cases of cyberbullying such as that carried out against Amanda Todd, ending in her suicide in 2012, make the point that of course it can be risky to reveal too much of oneself online. Over against these negative examples, however, there are numerous researchers who document what we can think of as positive privacy practices – including what Patricia Lange has described as two forms of «group privacy» on SNSs.

The first, the «publicly private,» is exemplified by posting videos on YouTube that are «hidden» in the sense that they are tagged in such a way that only close friends and relatives, as the intended audience of the video, know how to find them. The «privately public» goes further in terms of revealing to relatively unknown «friends» what a previous generation might have considered quite private, e.g. sexual orientation: but *not*, e.g. one's home address (Lange 2007).

Similarly, Stine Lomborg (2012) has documented how a prominent Danish blogger and her readers negotiate through processes of phatic communication the creation of a «personal space,» one that is neither purely individually private nor fully public. That is, the online exchanges often head in the direction of revealing more individually private matters: at the same time, especially when it becomes clear that a border has been crossed into what a given person feels should remain individually private, there is quick movement away from that discussion point back into a more neutral but shared space. As Lomborg puts it, «both author and readers balance a fine line between, on the one hand, pressure to reveal personal issues as a preamble for developing relationships among participants and, on the other hand, a norm of non-intrusiveness to protect each other's [individual] privacy» (2012: 432).

Lomborg's analysis is of particular interest precisely in that she argues that these communicative phenomena reflect Georg Simmel's notion of «the sociable self,» i.e. a self «engaged in a network of relationships» which as such is a self that «is attuned to the norms and practices within the network of affiliation» (*ibid.*). This is to say: the «personal space» that emerges through the blogger and her readers is precisely the sort of shared privacy («group privacy») that we would expect of more relational selves. In particular, it closely echoes the familial sense of privacy of traditional Thailand that we noted above (Kitiyidasai 2005).

Changing philosophical conceptions of privacy

In response to these transformations, there have been a number of efforts to reconceptualize privacy. The most significant of these is Helen Nissenbaum's account of privacy as a matter of «contextual integrity»: in this view, privacy emerges as a right to an «appropriate» flow of information as defined by a specific context (2010: 107 ff.). Such *contexts* or «spheres of life» can include, for example, education, the marketplace, political life, and so on. For a given context, a specific set of *informational norms* define the usual or expected flows of information *within* that context. These in turn are defined by three parameters: the actors involved (e.g. as subject, sender, and/or recipient); attributes (the types of information); and «transmission principles» that determine «the constraints under which information flows» (Nissenbaum 2011: 33). Nissenbaum gives the example of medical information shared between patients and their doctors. As highly personal and sensitive, patients expect this information to be kept confidential, though they would recognize that it could be appropriately shared with other medical professionals as needed. By contrast, were a physician to follow the informational norms of the market – e.g. by selling the information to a marketing company – patients' expectations of appropriate information flow «would be breached» and «we would say that informational norms for the health care context had been violated» (*ibid.*).

More broadly, precisely as Nissenbaum invokes *actors* as a first parameter defining information norms, she thereby cues us towards a now familiar sense of selfhood – namely, of human beings as taking up a wide range of roles and relationships with one another. Here Nissenbaum relies on James Rachels, who makes clear the connection between given *roles* – in his examples, «businessman to employee, minister to congregant, doctor to patient, husband to wife, parent to child, and so on» and specific expectations

regarding privacy (Rachels 1975: 328, cited in Nissenbaum 2010: 65, 123). So Rachels develops an account of privacy grounded in the recognition that «there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people» (Rachels 1975: 326, cited in Nissenbaum 2010: 65).

To my knowledge, neither Rachels nor Nissenbaum explicitly invokes a notion of selfhood as *relational* selfhood. But as Rachels brings forward the core importance of our social relationships as critical to defining privacy, he thereby clearly points in the direction of the relational or social selfhood we have seen theorized in Mead, Simmel, and Goffman, for example. This would suggest that Nissenbaum's notion of privacy as contextual integrity, resting as it does on the need to define actors and thereby on Rachel's attention to social relationships, is distinctively suited for the emerging emphasis we have seen on selfhood and identity as both individual and relational.

Relational selves and Internet research ethics: Successes (and failure) in the field

Implications for IRE?

These transformations in our practices and philosophical conceptions of privacy thus appear to closely correlate with the major shifts we first examined in some of our most foundational ethical concepts – namely, our conceptions of human identity and selfhood, as these in turn interweave with our understandings of ethical agency and ethical responsibility. We have also seen that extant forms of ethical guidelines for Internet research – apparently, with the exception of the NESH guidelines – presume an all but exclusively high modern conception of the individual as ethical

agent and all but exclusive bearer of ethical responsibility: these presumptions result precisely in primary obligations (whether utilitarian or deontological) to protect *individual* privacy, confidentiality, and so on. Clearly, as our sense of selfhood, ethical agency and responsibility, and correlative practices of privacy change, so our codes and guidelines for Internet research will need to change accordingly.

Again, it appears that the NESH guidelines, as enunciating most articulately and explicitly the requirement of researchers to protect not only the privacy (*privatlivet*) of individual subjects, but also that of their close relationships (NESH 2006: 17), thereby already demarcates the directions IRE will need to pursue in order to take on board these foundational shifts. At the same time, however, if we are to develop IRE codes and guidelines for these more recent practices and conceptions, our brief look at Nissenbaum's account of privacy makes at least one point clear: «privacy,» defined precisely in terms of the specific but widely diverse *actors*, roles and relationships that constitute selves as not simply individual but also as markedly relational, thereby becomes more complex, nuanced, and multi-faceted. In particular, we can characterize this shift in terms of a move *from* a relatively singular and stable understanding of the individual, and thereby relatively static or fixed conceptions of «privacy,» and thus what researchers were obliged to protect, *to* an understanding of the individual as strongly relational, where these multiple relations change over time. Thereby our conceptions of «privacy» become fluid and dynamic, as subject not only to specific *contexts*, but, more fundamentally, to ongoing negotiations between actors and their close circles of consociates (their *intimsfære*). Broadly, it seems that researchers' ethical obligations on this point will thereby become only that much more complex, dynamic, and, in some instances at least, very difficult.

Case studies

«Difficult,» however, does not necessarily mean impossible. On the contrary, three recent research projects using smartphones – i.e. devices that usually accompany us precisely into our most intimate and private spaces –exemplify some of the privacy challenges opened up not simply by current networked technologies, but by individuals who seem increasingly willing share intimate and private information across these networks. Two of these projects – one in Denmark and the second in the U.K. – appear to show that researchers can build privacy protections that are sufficiently strong to persuade their subjects that their personal information is safely held. A third example, however, shows that these new challenges are still sufficiently novel that extant guidelines, codes, and laws are not always able to provide researchers with needed guidance and support.

A first project, «Device Analyzer,» is based at the University of Cambridge, U.K., and, at the time of writing, has attracted the voluntary participation of over 17,000 participants worldwide (see http://deviceanalyzer.cl.cam.ac.uk/).[31] The purpose of the research is to discern patterns in how smartphones are actually used. Consistent with utilitarian approaches, the project website further elaborates the benefits that will accrue to participants. These begin with «new ways to look at what is happening inside your mobile phone!» – i.e. as the app records in exquisite detail more or less *everything* (more on this shortly) and makes this data, in both raw and analyzed forms, available to the participants. Specifically, the project's analyses offer to help participants choose the data plan (i.e. a given subscription or package of telephony and data services offered by a given provider, ranging from minimal minutes of talk,

31 (Accessed 14 March 2014). I am very grateful to Rich Ling (Telenor / IT-University, Copenhagen) for first calling my attention to this app.

numbers of texts, and megabytes of data downloaded – and thus least expensive – to more expansive and thereby expensive packages) best suited to their actual patterns of use as documented by these analyses, as well as apps that might be of interest. In addition, the project promises that «[t]his data is stripped of personally identifying information as best as possible while preserving useful information.»

Indeed, the project goes to great lengths to explain to participants how their individual identities are protected, coupled with a detailed list of the extensive range of data collected (see http://deviceanalyzer.cl.cam.ac.uk/collected.htm). Briefly, much of the data is «hashed» – i.e. assigned an identifier tag that refers, e.g. to a real number called by a participant: the project analyzes the tagged information, not the real numbers themselves, to discern, e.g. patterns in calling. Moreover, once the app is installed on one's phone, it provides participants with considerable control over the data collected (one can pause or stop altogether).The homepage is careful to inform the participant that «We do not collect transferred content. This means that we do not know which websites you visit or the login details that you enter.» This assurance is repeated in affiliation with specific components of the app – e.g. «Data transfer» – and in the descriptions of the details of the information collected (in this case, the amount of data transferred over a given period of time through either the phone connection or through WiFi).

At the same time, the kinds and amount of data collected are breathtaking: the detailed lists of data types alone fill more than one A4 page. It is distributed across four categories: basic data, data about applications and their use, hashed identification of the GSM cells the phone connects with, and an estimate of the phone's «coarse location» (every five minutes). And participants are clearly willing to contribute this data. While their identity may not be perfectly protected, it appears that participants are willing to have

this extensive and detailed data collected about their phone use both because they retain considerable control over their participation and because they receive some interesting and perhaps useful benefits. However this may be, the identity protections of the project are explicitly focused on *individual* identities (as hashed). It does appear that the identities of close friends and relations are also protected by default: phone numbers are hashed, for example.

A similar project on how Danes use their smartphones likewise requires participants to install a «Mobile Life» app, one that collects data such as «number of calls, sent and received text messages, location information, data usage, and product and application usage» (Zokem 2011: 1; author's translation). In this relatively extensive (four page) legal document, participants are promised anonymity: no personally identifiable information will be used (ibid.). Moreover, according to the project director, her participants are further assured by the fact that the project is sponsored by Telenor, which enjoys a strong reputation throughout Scandinavia.[32] As with Device Analyzer, the privacy protections offered here are squarely addressed to the *individual*. And, as with Device Analyzer, the content of messages, etc. sent to one's close associates is not collected. Moreover, the data collected are to be analyzed and distributed only in aggregated and statistical form, thereby protecting both the identity of the individual and the identity of those within one's *intimsfære*. In contrast with Device Analyzer, however, these protections are spelled out explicitly in terms of «rights and obligations» [*rettigheder og forpligtelser*] (Zokem 2011: 3), as defined by the national jurisdictions of Denmark and Finland (Zokem 2011: 1).

These two examples suggest that, so far at least, extant forms of privacy protections (e.g. hashing data and using only statistical

32 Christine Von Seelen Schou (Telenor & University of Copenhagen), personal communication, 20.12.2012.

aggregations) and relevant law (in the Danish example) are sufficient to assure contemporary subjects, addressed as *individuals* first of all, that the remarkable range of data recorded through their smartphones will not be used in ways that would reveal their identities and potentially embarrassing or harmful information about them. A last example, however, demonstrates that this is not always the case.

A proposed research project in Scandinavia was designed around the use of an app on participants' smartphones similar to the apps described above. The app would record the whole range of communicative behaviors facilitated through the phone, including texting, status updates, and web-browsing, photos taken and saved, contacts added, deleted and retained, and so on. This unprecedented glimpse into their subjects' personal lives – obviously a rich source of new research data – also presented now familiar ethical challenges regarding how to protect subjects' anonymity, privacy, and confidentiality. The researchers themselves were uncertain of how to proceed: worse, the various relevant authorities – their own university guidelines, national law and national research council guidelines – offered advice and direction based on earlier, more limited modes of research. The researchers thus faced a mix of both inappropriate and inconsistent guidelines. The result was, in effect, an ethical paralysis – with the further result that the research could not go forward.[33]

I suggest that these research examples are significant primarily because they (seek to) implement communication technologies that represent *par excellence* the extension of networked communications that both facilitate and symbolize our sense of selfhood as increasingly relational, not simply individual. The good news for Internet researchers who can only rely on extant guidelines is that research into our most intimate spaces and behaviors can go

33 Anonymous researcher, personal communication, 20.06.11.

forward nonetheless. This is in part as more traditional notions of individual rights to privacy are rigorously protected through technical means and, in the Telenor example, with an extensive legal contract. At the same time, insofar as we are indeed shifting in our sense of selfhood towards more relational selves, it may be that participants are willing to install such apps in part because of a somewhat greater comfort level with sharing personal information within research projects such as Device Analyzer that promise the «best possible» but not absolute individual privacy protection.

The collapse of the third project, however, suggests that current possibilities for Internet research that move into the most intimate spaces of our lives – a move that is coherent with increasingly relational senses of selfhood and more shared conceptions of privacy – are well ahead of extant guidelines, policy, and law in at least some cases. This collapse further suggests that Internet Research Ethics should pursue the development of new guidelines more precisely tuned to more relational senses of selfhood – though not necessarily at the cost of more traditional, individual senses of selfhood. In this development, we would likely be well served by taking up Nissenbaum's notions of privacy as contextual integrity as a starting point.

Concluding Remarks

Internet Research Ethics can now point to a long and deep tradition of both national and international literatures – including the AoIR and Norwegian National Ethics Committees' guidelines. But the relentless pace of technological development and diffusion constantly offers us new ways of communicating and interacting with one another – ways that frequently open up novel ethical challenges for us both as human communicants and as researchers. In particular, I have tried to show that a specific strand of challenges

emerge because of transformations at the most foundational levels, i.e. with regard to our primary assumptions regarding the nature of the self and thus how we are to understand moral agency, ethical responsibility, and affiliated notions of privacy – where protection of privacy stands as a primordial ethical obligation for researchers. To do this, I have traced important connections between the high modern ethical frameworks of deontology and utilitarianism with strongly *individual* notions of selfhood and privacy, as these have been foundational for IRE (and research ethics more broadly) over the past several decades. I have then turned to (late modern) shifts towards more relational conceptions of selfhood and affiliated notions of distributed morality and responsibility – as these correlate in turn with more recent expectations and practices of privacy as shared or group privacies, for example. Specifically, Helen Nissenbaum's account of privacy as «contextual integrity» draws specifically on more relational notions of selfhood – notions that we have also seen already explicitly in play in Norwegian approaches to privacy in terms of *privatlivet*, the *intimsfære*, and correlative Norwegian research ethics requirements to protect the privacy of not simply individual subjects but also that of the persons whose close relationships constitute the *intimsfære* and as such *privatlivet*.

Certainly, these shifts from more individual towards more relational understandings and practices of selfhood thus complicate and make more difficult the articulation and fulfillment of researchers' ethical obligations. But as both the extant Norwegian codes and the first two case studies explored in the final section suggest, «difficult» does not mean impossible. On the contrary, the success of these cases – of apps installed on smartphones that allow researchers to reach into what otherwise have been the most closed and intimate spaces of our lives – exemplify techniques, including articulate legal contracts, that appear to be viable and

effective in protecting both individual and more relational forms of privacy.

The failure of a third project, however, illustrates in part the fatal consequences for researchers in these new domains that can result instead when local guidelines and national codes fail to mesh effectively with these newer understandings and practices. Those of us engaged with the ongoing development of Internet Research Ethics obviously have our work cut out for us. I have argued that both the Norwegian research ethics codes and Nissenbaum's account of privacy as contextual integrity provide us both real-world examples and philosophical approaches that should prove most useful in such efforts.

References

Buchanan, E. and Ess, C. 2008. Internet Research Ethics. In K. Himma and H. Tavani (eds.), *The Handbook of Information and Computer Ethics*, 273–292. Hoboken, NJ: John Wiley & Sons.

Debatin, B. 2011. Ethics, Privacy, and Self-Restraint in Social Networking. In: S. Trepte and L. Reinecke (Eds.), *Privacy Online*, 47–60. Berlin: Springer

Ess, C. 2013a. *Digital Media Ethics*, 2nd edition. Oxford: Polity Press.

Ess, C. 2013b. Trust, social identity, and computation. In Richard Harper (ed.), *The Complexity of Trust, Computing, and Society*, 199–226. Cambridge: Cambridge University Press.

Ess, C. et al. 2002. Ethical decision-making and Internet research: Recommendations from the aoir ethics working committee. www.aoir.org/reports/ethics.pdf, accessed 14 March 2014.

Floridi, L. 2012. Distributed Morality in an Information Society. *Science and Engineering Ethics*. DOI 10.1007/s11948-012-9413-4.

Gergen, K. 2009. *Relational Being: Beyond Self and Community*. Oxford: Oxford University Press.

Giddens, A. 1991. *Modernity and Self-Identity*: *Self and Society in the Late Modern Age*. Stanford, CA: Stanford University Press.

Gilligan, C. 1982. *In a Different Voice: Psychological Theory and Women's Development*. Cambridge, MA: Harvard University Press.

Goffman, E. 1959. *The Presentation of Self in Everyday Life*. London: Penguin Books.

Habermas, J. 1981. *Theorie des Kommunikativen Handelns*. 2 vols. Frankfurt: Suhrkamp. (Vol. 1 translated as *The Theory of Communicative Action*, *Vol. 1: Reason and the Rationalization of Society*. Trans. Thomas McCarthy. Boston: Beacon Press, 1984. Vol. 2 translated as *The Theory of Communicative Action. Volume Two. Lifeworld and System: A Critique of Functionalist Reason*. Trans. Thomas McCarthy. Boston: Beacon Press, 1987.)

Hall, G. J, Frederick, D., & Johns, M.D. 2004. «NEED HELP ASAP!!!»: A Feminist Communitarian Approach to Online Research Ethics. In Johns, M., Chen, S.L., & Hall, J. (eds.), *Online Social Research: Methods, issues, and Ethics*, 239–252. New York: Peter Lang.

Hongladarom, S. 2007. Analysis and Justification of Privacy from a Buddhist Perspective. In S. Hongladarom and C. Ess (eds.), *Information Technology Ethics: Cultural Perspectives*, 108–22. Hershey, PA: Idea Group Reference.

Hursthouse, R. 2012. Virtue Ethcs. The Stanford Encyclopedia of Philosophy (Summer 2012 Edition*)*, Edward N. Zalta (ed.). <http://plato.stanford.edu/archives/sum2012/entries/ethics-virtue/>, accessed December 16, 2012.

Johnson, D. 2001. Computer Ethics (3rd ed.). Upper Saddle River, NJ: Prentice-Hall.

Kant, I. [1788] 1956. *Critique of Practical Reason*, trans. Lewis White Beck. Indianapolis: Bobbs-Merrill.

Kitiyadisai, K. 2005. Privacy Rights and Protection: Foreign Values in Modern Thai Context, *Ethics and Information Technology*, 7(1): 17–26.

Lange, P.G. 2007. Publicly private and privately public: Social networking on YouTube. *Journal of Computer-Mediated Communication, 13* (1: 2007), article 18. http://jcmc.indiana.edu/vol13/issue1/lange.html

Lomborg, S. 2012. Negotiating Privacy Through Phatic Communication. A Case Study of the Blogging Self. *Philosophy of Technology* (25): 415–434. DOI 10.1007/s13347-011-0018-7

Lü, Y.H. 2005. Privacy and Data Privacy Issues in Contemporary China, *Ethics and Information Technology*, 7(1): 7–15.

Mackenzie, C. 2008. Relational Autonomy, Normative Authority and Perfectionism, *Journal of Social Philosophy 39* (4, Winter): 512–533.

Markham, A. and Buchanan, E. 2012. *Ethical Decision-Making and Internet Research, Version 2.0: Recommendations from the AoIR Ethics Working Committee*, www.aoir.org/reports/ethics2.pdf

McCarthy, T. 1978. *The Critical Theory of Jürgen Habermas*. Cambridge: Hutchinson Press.

Mead, G.H. [1934] 1967. *Mind, Self & Society*. Chicago: Chicago University Press.

Natanson, M. 1970. *The journeying self: A study in philosophy and social role*. Reading: Addison-Wesley.

National Committees for Research Ethics in the Sciences and the Humanities (NESH), Norway. 2003. *Research ethics guidelines for internet research*. https://www.etikkom.no/In-English/Publications/Internet-research-/ accessed 14 March 2014.

The [Norwegian] National Committee for Research Ethics in the Social Sciences and the Humanities (NESH). 2006. *Forskningsetiske retningslinjer for samfunnsvitenskap, humaniora, juss og teologi* [*Research ethics guidelines for social sciences, the humanities, law and theology*]. http://www.etikkom.no/Documents/Publikasjoner-som-PDF/Forskningsetiske%20retningslinjer%20for%20samfunnsvitenskap,%20humaniora,%20juss%20og%20teologi%20%282006%29.pdf

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.

_____. 2011. A Contextual Approach to Privacy Online. *Daedalus*, *140* (4): 32–48.

Protection of Third Party Information in Research: Recommendations of the National Institutes of Health to the Office for Human Research Protections. 2001. http://bioethics.od.nih.gov/nih_third_party_rec.html

Rachels, J. 1975. Why Privacy is Important. *Philosophy and Public Affairs* 4(4): 323–333.

Simmel, G. 1955. *Conflict and the web of group affiliations*. New York: The Free Press.

_____. 1971. Sociability. In D.N. Levine & Simmel Georg (Eds.), *On individuality and social forms. Selected writings* (pp. 127–140). Chicago and London: The University of Chicago Press.

Simon, J. 2013. Distributed Epistemic Responsibility in a Hyperconnected Era. *The Onlinfe Initiative*. https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Contribution_Judith_Simon.pdf

Stahl, B.C. 2004. *Responsible Management of Information Systems*. Hershey, Pennsylvania: Idea Group Inc.

Tavani, H. 2013. *Ethics and Technology: Ethical Issues in an Age of information and Communication Technology*, 4th ed. Hoboken, NJ: Wiley.

Taylor, C. 1989. *Sources of the Self: The Making of the Modern Identity*. Cambridge, MA: Harvard University Press.

UCLA OHRPP (Office of the Human Research Protection Program, University of California, Los Angeles). 2011. Guidance: Secondary Subjects. http://ora.research.ucla.edu/OHRPP/Documents/Policy/9/Secondary_Subjects.pdf

Vallor, Shannon. 2009. Social Networking Technology and the Virtues. *Ethics and Information Technology*. 12 (2), 157–170.

_____. 2011. Flourishing on facebook: virtue friendship & new social media. *Ethics and Information Technology*. 14(3), 185–199.

_____. 2012. Social Networking and Ethics. *The Stanford Encyclopedia of Philosophy* (Winter 2012 Edition), Edward N. Zalta (ed.), forthcoming URL = http://plato.stanford.edu/archives/win2012/entries/ethics-social-networking/.

Willson, M. 2010. The possibilities of Online Sociality. In J. Hunsinger, E. Klastrup & M. Allen (eds.), *International Handbook of Internet Research*, 493–506. New York: Springer

Zokem Ltd. 2011. Fortrolighedspolitik og Deltageraftale [Privacy Policy and Participant Agreement], Telenor Smartphone undersøgelse [study] 2011. http://www.wilke.dk/telenorpanel/Deltageraftale_Telenor.pdf

Researching social media: Confidentiality, anonymity and reconstructing online practices

Marika Lüders
SINTEF ICT
marika.lueders@sintef.no

Introduction

In only a matter of years, people have populated online spaces in ways that interweave us in mediated spheres as part of our lived realities. We live in screens and in the intersections between screens. Many of these spaces are public and semi-public. At first glance, personal practices in these spaces might appear at odds with the public character of the venue: yet self-presentational strategies and interactions become more meaningful when we share actual traces of life. The concept of privacy is hence a moving target, constantly being negotiated and renegotiated as a consequence of how we perceive the in-flux boundaries between public and private spheres. And not only is our personal life closely integrated with mediated practices. Professional life is increasingly moving online, with the emergence

of social intranets attempting to replicate social network sites within enterprise contexts.

In this paper, I will discuss how we can research mediated practices, both personal and professional, without compromising the privacy of the people being studied. One core premise is that the potential public character of the content and people being studied does not warrant the public display and exposure of the research subjects. Traditional research ethics, ensuring the privacy of the research subject, remains key, and perhaps ever more so.

I have conducted several studies on how people make use of the Internet in their everyday life for personal matters, as well as in organizational work and professional and work-related domains. Two different qualitative studies will be presented as examples, demonstrating why researchers need to tread carefully when approaching research subjects, gathering data, and presenting results in publications. The first example is taken from a study of young people's use of social media, and is based on interviews of 20 young people between 15 and 19 years of age, as well as on observations of their online practices in blogs and social network sites (SNS) in the years 2004–2007. The second example is taken from a study of the use of a social intranet in an international ICT consultancy enterprise. This study was conducted in the years 2010–2013, and is based on interviews with 27 employees as well as on analyses of their social intranet user patterns. In the latter example, the social intranet is only available for the company employees, and the content studied cannot be republished in research publications. In both examples, the informants being interviewed gave their informed consent to participate, and were guaranteed anonymity, complying with requirements and procedures for data handling as defined by the Privacy Issues Unit at the Norwegian Social Science Data Service (NSD).

In the following pages, I will first briefly review relevant literature on mediated practices and the specific challenges this poses for research. I will then discuss the particular research challenges experienced in studying social media practices in personal and professional contexts, before concluding with a discussion of the consequences of blurred private/public/professional realities for qualitative research.

Background: Researching online practices

Traditional research ethics stipulate certain requirements regarding how research should be conducted (for example, participants should be informed about the purpose of the study, that participation is voluntary, and that they can withdraw from the study at any time). Only then can the participants give their informed consent to participate. The requirement to obtain informed consent from research participants is incorporated in European legislation (European Commission, 2013: 14). For Norwegian research projects, the Privacy Issues Unit at the Norwegian Social Data Service (NSD) ensures that research projects, including the recruitment of participants and the management of personal data, are conducted according to Norwegian privacy laws. The unit ensures that the collection, safeguarding, storage and reuse of personal data comply with ethical and legal standards.

Yet, whereas traditional research ethics may seem relatively uncomplicated, challenges arise for researchers who attempt to understand and analyze online personal practices, particularly when it comes to republishing online content in research publications. When discussing research of online behaviour, we need to discuss the character and perceptions of online behaviour as situated between the always renegotiated spaces between what is private and what is public.

Overall, the dual notions of online/offline tend to keep us focused on the differences between online and offline rather than on the embodied realness of online behaviours. Addressing online/offline is preferable to the «old» dual notions of virtual/real, yet we need to improve our understanding of online life as an integral part of life. Users' behaviour online is usually «firmly rooted in their experience as embodied selves» (Ess, 2003: 26). Similarly, Nissenbaum (2011: 43) argues that life online is thickly integrated with social life, and that online practices «retain fidelity with the fundamental organizing principles of human practice and social life». Thus, norms governing the sharing and distribution of personal information remain key even for social life online (ibid.). From this we can assume that research on mediated practices should comply with conventional research ethics.

In a Norwegian context, the NESH guidelines for research ethics stress the importance of the researcher considering people's perceptions of what is private and what is public (Bromseth, 2003, Forskningsetiske komiteer, 2006: 17). For example, reader debates in online newspapers are manifestly public. Observations of public offline settings usually do not require consent from the observed subjects, who remain unknown and anonymous to the researcher (Mann, 2003). Similarly, following the first version of ethical guidelines for Internet research published by the AoIR ethics working committee, «the greater the acknowledged publicity of the venue, the less obligation there may be to protect individual privacy, confidentiality, right to informed consent, etc.» (Ess, 2002: 5).

However, assessing the acknowledged publicity of an online venue is not always straightforward, at least not as seen from the point of view of the participants. A personal blog might be publicly available for all to read, though very often it can be regarded as a personal and private space by the author. As a researcher I typically inform study participants that personal data will be anonymized and that it will not be possible to identify who they are.

This means that I cannot republish online content originally published by research participants even if that content is publicly available online. The fact that people publish personal information online, and leave publicly available traces of sociability and self-performance, does not mean that this content is «up for grabs» by social scientists without carefully considering the privacy of the people being studied. As emphasized in a number of studies, people may maintain strong expectations of privacy and ownership of personal data even if that data is in fact publicly available (Walther et al., 2008, Lüders, 2011, boyd and Marwick, 2011). Other online spaces are manifestly restricted in terms of publicness and are only accessible by invited and registered users. Private Facebook, Twitter and LiveJournal profiles as well as company intranets and online resources should leave no researcher in doubt as to whether they can use this content in their own publications. They cannot, at least not without consent and anonymizing the content.

Much has changed since the publication of the first version of ethical guidelines for Internet research by AoIR in 2002. As a consequence of technological developments, a new version of the guidelines was published in 2012 (Markham and Buchanan, 2012). These guidelines propose that a number of principles are fundamental to an ethical approach to Internet research. First of all, the researcher needs to consider the vulnerability of the people being studied. The greater the vulnerability, the greater the obligation of the researcher to protect them. Secondly, a one-size-fits-all approach is not viable. Harm is defined contextually, and assessing how to conduct ethically sound research must be made according to the specific context. Thirdly, digital information involves individual persons even if it is not immediately apparent how and where persons are involved in the research data. Fourthly, the rights of subjects may outweigh the benefits of research. Fifthly, ethical issues may arise during all steps of the research process. Ensuring that the privacy of

the people being studied is not compromised is therefore important in all stages of the process, from planning to publication and dissemination. Finally, the guidelines stress ethical decision-making as a deliberative process, meaning that researchers must consult as many people and resources as possible in this process.

I will return to some of these principles in the conclusion, addressing how two different studies require certain strategies for ensuring the privacy of the research participants.

The two case studies I will discuss are similar in that I rely on interviewing people in addition to studying their online practices. As the participants have agreed to take part in the study on the condition that their identity will not be revealed, I do not include explicit examples of content they have published online. Protecting the privacy of my informants concerns how I gather and store data, as well as how I refer to them and their online practices in publications. As will be evident, a consequence of the agreement with the informants is that any empirical examples of content must be reconstructed, even if this practice is scientifically disputed. Reconstructing empirical examples does not imply inventing examples, but making required changes in order to maintain the original meaning and message while ensuring the original content cannot be retrieved through searches.

Example 1: The use of social media among young people

In my PhD work I followed 20 people between 15 and 19 years of age in the period 2004–2007. I followed their online practices in their blogs and in social network sites, and I interviewed all of them once. My informants were guaranteed anonymity, and their names were changed in the analyses and publications. These conditions were described in a formal postal letter of consent, which the

informants signed. According to the Norwegian Data Inspectorate (Datatilsynet), minors who are 15 years or older can give their informed consent in the relevant sort of cases (Datatilsynet, 2004).

My study concerned mediated individual practices, some of which could expose the informants in rather intimate ways (e.g. revealing photos or textual confessions) and disclose their identity if republished in the context of this thesis. Though these expressions were often publicly available online, efforts were made to secure the privacy of the informants. I reported on their online lives and user patterns, but I did not republish their online expressions or photos.

At that time, young Norwegian bloggers typically avoided revealing their full name in their blogs and/or protected all or part of the content as accessible only to connected blog friends (e.g. with friends-only blogs in LiveJournal). Hence you could not google my informants and find their blogs. Yet those with publicly available blogs were all easily recognizable if you found their blogs and knew them offline: they revealed their first names, and often published pictures and other information that exposed their identities. My obligation to ensure the anonymity of my informants meant I simply could not include any information that might identify them. My inability to include content which my informants had created online was thus a consequence of conducting research interviews. It was simply not viable to combine anonymous interviews with analyses of online practices if those practices were also reproduced in my work.

However, even if a researcher relies only on analyzing online content (and thus avoids the problem of revealing the identity of interviewees who have been promised anonymity), the public availability of content does not necessarily imply that content can be used without consent, or at all. We need to consider people's perceptions of what is public and what is private. The experiences and perceptions of my informants illustrate the complexities involved.

Informants who had a publicly available presence (even if anonymous or pseudonymous) perceived these spaces as private. They did not regard their blogs as public by practice, even if the blogs indeed were public by technology. The development of media technologies has always been connected to the increasing exposure of the private sphere in the public sphere (Warren and Brandeis, 1890: 195, Barthes, [1980] 2001: 119, Meyrowitz, 1986: 99). Network cultures reinforce this tendency. In public contexts people generally act in accordance with the expectations of several other groups (Meyrowitz, 1986). Even so, personal blogs and social profiles can be perceived as private, even when they are publicly available:

> Kristoffer (18): For a long time I had a title on my blog saying that if you know me, don't say that you have read this.
>
> Marika: Why?
>
> Kristoffer: Because then it would affect what I write. Then I would begin to think in relation to that person. I try to write my thoughts, but if I know that a person is reading it I begin to think of that person as a recipient. And I just want my message to get across; this is my message to myself.

18-year-old Linnea describes a similar experience with her blog as her own private space:

> Linnea (18): I try to pretend that no one reads it. Or that I should be able to be honest and write what I want to without thinking, no, I can't say that because he will read it and I can't write that because she will read it and I definitely can't write that because the whole class will read it.

In spite of the fact that Linnea, like Kristoffer, emphasizes that she cannot consider her readers when she writes, she does appreciate having readers and is happy and grateful when she meets people who have followed her life through her texts and photos: «I think

that if the diary is worth spending time on, then I am doing something good. […] And that I can mean something to someone. That feels really good.» Kristoffer and Linnea publish texts and photos online because they enjoy writing and taking photos, and they appreciate comments from readers.

The interviews demonstrate the indeterminate distinction between the private and public subject, and also pinpoint how offline as well as online publics include private spaces:

> Kristian (17): After all, the Internet is no more public than the world outside […]. I don't care if a stranger sitting at the next table in a Chinese restaurant eavesdrops on my personal conversation with a friend.

The Internet is more public to the extent that actions are available to an audience independently of time and space: i.e. expressions stretch beyond the here and now, as is the case for public blogs, social profiles and photo sharing services. All the same, Kristian does have a point that often seems to disappear when distinctions between private and public arenas are discussed: private actions take place within public spaces both online and offline. My informants thus perceive the Internet as a public space, but in this public space they create their own private spaces where they share personal narratives and experiences. Worrying that personal information published online can be misused is characteristic for dominant societal discourses, also affecting the perceptions of the informants. Simultaneously, they regard having a public presence online as meaningful and valuable. My informants often appeared surprisingly honest online, but they typically emphasized that they negotiated what they shared, as they were well aware that their blogs were publicly available. Fifteen-year-old old Mari explains, «I only share a little bit of myself with the rest of the world, not everything».

Although I did not include content published by my informants in my publications, I did include extracts from other «typical» teenage blogs and profiles, but I chose to reconstruct them, and I got their informed consent to publish the content in my own work. One of the extracts I included was a blog post by 17-year-old Mari. She writes mainly friends-only posts in her LiveJournal, available only for users she has added to her friends list. Occasionally she makes exceptions and writes public posts, and I used one of these posts to illustrate how she negotiates boundaries between her private and public self-performance. I first translated her blog post to Norwegian for a Norwegian publication. I then translated it back to English for my thesis. I also googled different parts of the quote to make sure her blog could not be retrieved based on the reconstructed post in my own work. This does mean that my research becomes less traceable, though I reconstructed her blog post to keep Mari's identity anonymous:

> The first time we kissed was at the traffic lights near Hyde Park. I was still sort of in a state of shock and giggled and laughed at what he said without saying much myself. To be honest I was quite frightened by the weirdness of the situation. My Internet friend had come out of the screen and as always when that happens, my brain and ability to formulate do not cooperate particularly well.
>
> So there we are waiting for the green man and he has his arm around me and I lean in to him and try not to pass out from all of these new experiences and I look up at him and smile (something which in itself is nothing new – I always smile) and he looks at me and leans towards me and we kiss. I get a bit funny inside but I do not gasp, and it is actually not unbelievably romantic. […] We kiss affectionately with open mouths and then the green man appears and we stop kissing and we giggle a bit before we move across the road while still closely entwined. («Mari's blog post»)

It may seem contradictory that Mari chooses to air a rather private experience in public; however, in an e-mail she explains that she chose to make this post public, because «it's about a very important and positive event in my life, and I managed to write something nice and reasonably meaningful». In continuing she explains that she is satisfied with how she manages to present herself and her personality, and that she wants to share this story because she knows that numerous others identify with «Internet romances». In this way, online spaces are used to mediate personal experiences and bring what is private into public spaces.

My informants stressed that they felt they had personal control over mediated expressions, meaning they could carefully create expressions that they were comfortable sharing. The consequence of this perceived sense of control implied they would share stories online that they would not typically share with their friends offline:

> Andreas (18): It's easier to express yourself accurately online, so online conversations are often profound and very open. You can write it down, and have a second look at what you're trying to say. If you don't like how you expressed something, you can just edit it. Then it's easier to be honest, and I think it's easier to tell people what I really feel.

Most of the texts and photos that Andreas (18) publishes are publicly available. Private revelations, however, are only available to registered friends or acquaintances (i.e. people added to his friends lists). Yet occasionally he needs time to decide what he wants to share with others:

> Andreas (18): You kind of want to get it out, but you don't want anyone to know just yet, so it is good to be able to write a private post. Even if I have a tendency to make private posts available to friends when I read them the day after.

Anders (17) writes a paper diary in addition to his online diary: «I'm more open and honest in my diary, but on the whole what I write in my diary comes out on LiveJournal a couple of days later. I just need some time to think and such.» The comments of Andreas and Anders indicate that the opportunity to construct expressions and to be able to reconsider these expressions at a later point sometimes make them present themselves differently in mediated settings. Similarly, the physical absence of others makes users feel more in control of their mediated sense of self, or in Goffmanian terms, users have more control with expressions given off (Goffman, [1959] 1990: 210–212).

In other words, there are unique qualities with mediated forms of communication, and these qualities affect how individual users choose and manage to present themselves. Thus mediated communication is sometimes characterized by candidness, as users have more time to create expressions and exercise greater control over self-representations.

To summarize, Internet services such as blogs and SNSs are peculiar: although technically they might be public or semi-public, these spaces provide us with an opportunity to be publicly private in modes we have not previously been accustomed to. We can inhabit them and share experiences in the form of texts and photos with an audience that stretches far beyond what used to be possible in pre-Internet times. Yet my informants were very clear about their limits of intimacy. The online subject can be open and honest, often more so than in offline sociability, yet what is made available remains a filtered reflection of the self. Most importantly, the ambiguity of blogs as private or public means that «technically public» does not equal «public in practice» or «public» as content that researchers can choose to use as they please.

Example 2: The use of a social intranet among knowledge workers

The second case study I will discuss with regard to research ethical assessments is a qualitative in-depth study of the adoption of the social intranet Jive Software by an international ICT consultancy enterprise that employs approximately 5,000 people. The study, involving qualitative interviews with 27 employees located in four different countries and observations of user patterns in the social intranet, was conducted by Lene Pettersen and myself.

Consultants in all divisions of the enterprise are typical knowledge workers, and the company introduced JIVE in the summer of 2010 to enable employees to «build professional networks, develop competence by following others more skilled, finding out what others are doing and not reinventing the wheel, having things you're working on easy to find and share, easily work with colleagues in other business units» (obtained from the company's strategy for implementing JIVE). JIVE has been organized as a social intranet tool, with national as well as public intranets and restricted groups for discussions and sharing of content, experiences and knowledge. The newsfeed that the employees see when they log in depends on which office they belong to, which peers they follow, and which groups they have joined as members (i.e. similar to how Facebook and LinkedIn function).

As used by our case company, JIVE is a non-public space: online practices are only available to the employees in the company. As such information is not public. In this study, protecting the privacy of our informants proved to be very important. In the course of the research process we also realized we had to keep the company anonymous in order to report as truthfully as possible what our informants told us. When conducting qualitative research projects, the aim is often to uncover in-depth knowledge about experiences

and opinions as truthfully as possible. To succeed, researchers need to develop trust and rapport with the interviewees.

In our study, we soon experienced the benefits of having established a relationship of trust with our informants. They were informed about the study being conducted without disclosing their identity to the company or anyone else. Information about handling of data was included in the information about the study that the informants received before giving their informed consent to participate. This letter also described that the study had been reported to the Norwegian Social Science Data Services, and that the study and the handling of empirical data was conducted in compliance with its regulations with regard to confidentiality and archiving of data. It would not be possible to recognize the persons interviewed in any reports or articles. This formal procedure for guaranteeing that the study would ensure our informants' confidentiality and privacy seems to have helped us to establish rapport and trust. We experienced a high level of candidness from our informants, as demonstrated by highly opinionated expressions about the company, the social intranet and their local work environment.

In the past few years, the company had faced a series of acquisitions, reorganizations, and a significant labour turnover, resulting in frustration for some informants. The interviews we conducted provided us with in-depth insight into the workplace experiences of our informants. The openness our informants showed us demonstrates the importance of having established a trustful relationship.

> No, as I said earlier, our culture has changed significantly. When I started […] everyone had their own voice and were individuals with their own opinions. This has changed. Now we're supposed to brown nose those with many important and international contacts and who might be promoted to

> an important position. [Those who participate extensively in JIVE] are those who try the hardest to position themselves. […] Their billable time is minor, and they talk a lot [laughs]. (Female in her 40s)

All is not misery in our case company: there are distinctive differences between the informants, and also differences in the experience of the work environment at local offices, and the quote above is representative only for the above informant. Yet her opinions are reflected in more modest forms among other informants as well:

> [Active users of the social intranet] are the Yes-people. Those who flatter and agree with the management. The Yes-people are those who participate in the social intranet, and who reproduce their Yes-views in their Yes-clan (male in his 30s).

This input is crucial when we try to understand the employees' experiences of the company's social intranet. The honesty our informants showed us made them more vulnerable, and making sure they could not be identified by the company or anyone else became even more essential to us. Moreover, conducting the interviews uncovered that reluctant users of the social intranet had significant privacy concerns: for example, they would not «like» critical posts by colleagues even if they actually liked the content, because their own name would then be visible to everyone in the company, including managers (Pettersen and Brandtzæg, 2012: 13–14). Conversely, the experiences and opinions of informants who actively participate with content in the social intranet could also increase the vulnerability of informants if their identity were disclosed.

> I think you can use JIVE to brand your name within the organization. I'm not saying I'm schmoozing with the management […]. But with JIVE […] like when I comment on a post from [manager], the distance between us decreases and my

> name might be noticed. […] There were no similar opportunities before JIVE. Like I couldn't keep track of what my manager was thinking and feeling, and then e-mail him and say, «Hey, I really like what we're doing now». (Female in her 30s)

Our promise to keep the informants anonymous both for the company and for the public means we avoided providing information about the office they belong to and their specific age, and we removed any information that might identify them. Gender and approximate age are included, as in the examples above: «female in her 40s». The combination of information about gender, specific age and office can easily reveal who many of them are. We carefully and consistently assessed whether the information we included in publications contain information that could result in individuals being identifiable. This is of course particularly important as our informants have shown us a level of trust and told us stories that might jeopardize their professional position in the company and even future positions if they choose to pursue a career elsewhere.

In this study, our responsibility to our informants makes it more challenging to present JIVE in a meaningful way to readers who are not familiar with the service, i.e. most readers. Screenshots of how the company makes use of JIVE cannot be included as is, but must be manipulated to protect both the company and the users. In her work, Pettersen has manipulated screenshots from the company's social intranet, substituting fictional photos and names for real photos and names in order to visualize the technical solution (for illustrations, see Pettersen and Brandtzæg, 2012). This practice resembles what Markham (2012) has labelled «fabrication» of empirical data. As Markham explains, within scientific communities «fabrication» of data is typically regarded as unethical research conduct. Yet, considering the need to protect the privacy of individuals when conducting qualitative studies of online practices, Markham claims fabrication is a sensible and ethically sound way

out. Instead of including empirical examples as is, the researcher instead creates composite accounts of persons, events or interactions. Fabricated examples are hence ideal type descriptions induced from the material. Such research practices are still scientifically disputed, and the need to protect the privacy of informants might jeopardize opportunities to get published. As Markham explains with reference to another case,

> I learned that a publisher had rejected a paper written by two of my colleagues, solely on the claim that they were faking their data by presenting invented composite blogs instead of quoting directly from actual blogs. (Markham, 2012: 334)

Similarly, Pettersen and I have received reviews of our work that express concern about the lack of detail about JIVE: «A first concern is the lack of detail we have on JIVE – its particular functionality – screenshots and so forth might be useful» (from a review on a paper submitted to a conference). Pleasing reviewers would require us to reconstruct, in greater detail, screenshots with fabricated textual and visual content to protect the anonymity of the company and the employees, which in turn might prompt reviewers to criticize the illustrations as fake and constructed.

To summarize, researching non-public company websites that contain confidential information requires specific considerations with regard to how the researchers treat the research subjects. Clearly, content cannot be published as is. However, also information retrieved through research interviews must be handled carefully. Our informants trusted us, and several informants shared stories they would not share publicly in the company. The relation between trust and sharing is of course well documented in several studies, and is also something we as researchers benefit from. As a consequence we cannot share information or *combinations of information* that might harm our informants if they are made

recognizable. We can consequently relate our experiences with arguments that point towards the need for fabricating or reconstructing data in ways that protect informants, even if such reconstructions might be at odds with requirements about how research results are usually presented.

Conclusion

The informants in the two case studies are vulnerable, but for different reasons. Young research participants are vulnerable due to their age. In my study of young people's online practices, my informants were also vulnerable as a consequence of their self-performance practices in social media. Even if their blogs were publicly available, they still perceived their own blogs as their own private space and disclosed honest and intimate (if nevertheless filtered and edited) accounts of life. The interviews were conducted on the condition that the participants would remain anonymous, and this made it impossible to include content from their online practices in research publications. The knowledge workers interviewed in the second case study are adults with a high level of social, cultural and economic capital. However, most of our informants made themselves more vulnerable by sharing experiences and opinions they would not share openly in the company. They felt comfortable doing so because they trusted us to keep their identities anonymous.

Both case studies demonstrate how a one-size-fits-all approach with regard to ethical decision-making is not viable. The peculiarities of each case are only uncovered in the actual research process, and consequently the premises for making ethically sound judgments changed during the course of the studies. The interviews with the young bloggers uncovered complicated perceptions of private versus public, which only emphasized how I could not possibly

use their content as I pleased in my own work. Similarly, Pettersen and I entered the social intranet case study rather naively, thinking it would suffice to keep the identity of the informants anonymous. The stories we heard are typical for knowledge workers, yet we could only report these stories truthfully if we also kept the identity of the enterprise anonymous. In both cases, ethical issues arose throughout the research process. Moreover, both case studies point to the importance of thinking in terms of ethics throughout the research process, from planning to publication and dissemination. Strategies to ensure the privacy of the research participants, for instance, instilled creativity concerning ways of illustrating online practices. These could not be republished as is in publications, but had to be anonymized and reconstructed even if such reconstructions might be at odds with «normal» scientific practice.

A process approach to research ethics means that the particular judgments made in the above case studies cannot easily be applied in other research cases. Ethical challenges will arise at different stages in the research process, and many of these challenges will only become apparent as the researcher becomes embedded in her research project.

References

Barthes, R. [1980] 2001. *Det lyse rommet: tanker om fotografiet [Camera Lucida: Reflections on Photography]*, Oslo: Pax forlag.

boyd, D. & Marwick, A. 2011. Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*. Oxford Internet Institute.

Bromseth, J.C.H. 2003. Ethical and methodological challenges in research on net-mediated communication in a Norwegian research context. *In*: THORSETH, M. (ed.) *Applied Ethics in Internet Research* Trondheim: Programme for Applied Ethics, Norwegian University of Science and Technology.

Datatilsynet 2004. Barn og unges personopplysninger: Retningslinjer for innhenting og bruk. Datatilsynet.

Ess, C. 2002. Ethical decision-making and Internet research. Recommendations from the AoIR ethics working committee. Association of Internet Researchers.

Ess, C. 2003. Beyond *Contemptus Mundi* and Cartesian Dualism: the BodySubject, (re)New(ed) Coherencies with Eastern Approaches to Life/Death, and Internet Reserach Ethics. *In*: THORSETH, M. (ed.) *Applied Ethics in Internet Research*. Trondheim: Programme for Applied Ethics, Norwegian University of Science and Technology.

European Commission. 2013. Ethics for researchers. Available: http://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf.

Forskningsetiske komiteer 2006. Forskningsetiske retningslinjer for samfunnsvitenskap, humaniora, juss og teologi.

Goffman, E. [1959] 1990. *The presentation of self in everyday life*, London, Penguin Press.

Lüders, M. 2011. Why and how online sociability became part and parcel of teenage life. *In*: CONSALVO, M. & ESS, C. (eds.) *The Handbook of Internet Studies*. Oxford: Wiley-Blackwell.

Mann, C. 2003. Generating data online: ethical concerns and challenges for the C21 researcher. *In*: THORSETH, M. (ed.) *Applied Ethics in Internet Research*. Trondheim: Programme for Applied Ethics, Norwegian University of Science and Technology.

Markham, A. 2012. Fabrication as ethical practice. *Information, Communication & Society*, 15, 334–353.

Markham, A. & Buchanan, E. 2012. Ethical Decision-Making and Internet Research. Recommendations from the AoIR Ethics Working Committee (Version 2.0). Available: http://aoir.org/reports/ethics2.pdf [Accessed 6. May 2013].

Meyrowitz, J. 1986. *No Sense of Place: The Impact of Electronic Media on Social Behavior*, New York, N.Y., Oxford University Press.

Nissenbaum, H. 2011. A Contextual Approach to Privacy Online. *Daedalus*, 140, 32–48.

Pettersen, L. & Brandtzæg, P.B. Year. Privacy challenges in Enterprise 2.0. *In*: Internet Research 13, 2012 Salford, UK. AoIR.

Walther, J.B., Van Der Heide, B., Kim, S.-Y., Westerman, D. & Tong, S.T. 2008. The Role of Friends' Appearance and Behavior on Evaluations of Individuals on Facebook: Are We Known by the Company We Keep? *Human Communication Research*, 34, 28–49.

Warren, S. & Brandeis, L.D. 1890. The right to privacy. *Harvard Law Review* 4.

Counting children

On research methodology, ethics and policy development[34]

Elisabeth Staksrud

Department of Media and Communication,
University of Oslo

elisabeth.staksrud@media.uio.no

Introduction[35]

One of the challenges we often face as researchers within the social sciences and humanities is to answer the question concerning how our research can contribute to society at large. What is the relevance of what we do? Can we make people's lives better? Safer? More manageable? A typical way of ensuring – or

34 This contribution is in part built on Staksrud (2011). The data that forms most of the empirical basis and experience for this chapter originally derived from the general social sciences exercise of producing quantifiable results to inform policy making, and the tension and interaction that often rapidly erupts between moral panics, policy development and academic research. The data was not originally collected for research purposes, but with the intention of informing policy and pinpointing effective practical strategies for online safety work. It was not based on a theoretical model, but developed as a co-generative study, with «everyday theorists» (Bruhn Jensen, 2002, p. 287).

35 In this paper, the distinction «quantitative – qualitative» is used literally, not derivatively.

providing – such relevance is by informing policy development. As we all know, the global nature of the Internet creates challenges for policy makers. The Internet, with its content, risks, services and users, is in essence trans-national – and even global. Its basis is not governments, but rather commercial companies, private citizens, and organizations. At the same time most societies, on a political level, need and want to keep services and businesses in line with current policy developments and to ensure the moral and legal rights of citizens, in this case users. This relates both to rights of protection from potential harm and illegal content and the right to communication and activities whose status depends on legal, societal, cultural and financial frameworks, conventions and expectations. For instance, pornography and violent content can be (legally) published in one country and accessed by users – young and old – in other countries, where the content is deemed illegal. Likewise, a paedophile can groom a child anywhere in the world, and a teen can illegally download copyrighted material from a server or network situated on the other side of the planet.

Traditionally, a practical way of solving the legal challenges that the Internet's seemingly borderless nature creates has been to implement and rely on self-regulatory agreements where commercial companies take on social responsibility (Staksrud, 2013, pp. 87–110). Thus, for the users their rights as traditionally afforded by the nation-state are transformed into user agreements for the use of the technology, typically labelled «rules of conduct» or «terms of service». However, unlike nation-states, commercial companies do not have evaluation, transparency and accountability built into their organizational structures. Consequently, independent testing and evaluation becomes the cornerstone of all self-regulatory policy efforts. With the ethical and methodological safeguards that are built into the trade and traditions, researchers can help fulfil

this need for accountability and transparency, and may do so with both local and territorial/global perspectives.

Doing so, the researcher must look beyond standard modes of operation in order to fulfil obligations on all levels. Despite them being obvious points, one must actually heed the fact that online activities are cross-border, one must consider ethical aspects such as the question of whether gathering information may be problematic even if the data is freely available, and one will have to consider commercial interests to a perhaps greater degree than the usual political ones.

Building on this understanding, this chapter addresses three methodological and ethical challenges related to Internet research:

1) How can we make sure that we do not replicate standard perceptions of minors' Internet use, but rather open up the field to gain new insights?
2) How can we research communicative features and user practices in online communication services, such as social networking sites, without compromising the privacy and integrity of third party users, especially when these users are children?
3) How can we as researchers fulfil our mission of independence and critical reflection on policy development in a field where businesses rather than governments are the principal regulators?

The challenges will be addressed by making it even harder: Critical policy research in online environments is challenging in itself due to the new and complex array of stakeholders and the lack of transparent regulatory frameworks. It is even harder when the users in question are minors (children), often assumed to be «vulnerable» users, with all the added ethical complications and obligations this entails. Throughout the discussion, «children» will be used as the Internet user and informant of reference.

The right to be researched

Perhaps the biggest challenge in the quest to ensure people's right to be researched is to research underrepresented, so-called «vulnerable» groups. These are groups for which informed consent cannot be obtained directly and sufficiently, e.g. people with mental disabilities, those with financial needs that might make them vulnerable to certain types of research (having no real choice to opt out), or – the largest group of them all: children. For all of these groups there are special ethical considerations, which place a larger responsibility on the research community as a whole. For in a risk society, as described by Farrell (2005, pp. 2–3), research with children is in itself understood as a risky enterprise, and stringent legislation and policies are designed to protect children from dangerous adults – including researchers (see also David, Tonkin, Powell, & Anderson, 2005).

An unintended but yet real result of this state of affairs is that one often finds these groups less researched than others. This is especially the case when we look at issues related to the «population», the «public», or, as typically within the research field of media and communication, the «audience» or «users». Children constitute a prime example of a sub group which is often (if not always) forgotten, and in reality are overlooked when it comes to sampling and collection of data that aims to inform policy development in general, and policy related to children themselves in particular. Therefore, in policy as in research, when we refer to «the public» and its features, forms, needs and meanings, we often do not mean all people, but rather those above the age of 15 (at best), or more likely above 18.

Traditionally, to the extent that children are researched, this has typically been done by proxy, by asking their parents and guardians about how they are, what they do and how they feel. Even when comparing *children*, this is often done, explicitly or implicitly, by using

adults and their behaviour and experiences as a frame of reference providing the desired standard. As noted by Livingstone (2003: 158), researchers are less likely to ask children directly about their access and use, and more prone to ask their parents. Thus, much quantitative research and surveys on children in general and their media practices in particular have not been conducted with children, but rather with their parents, who assess and report on how their children behave, feel and (to a lesser extent, see Staksrud & Livingstone (2009)) *cope* with various issues (see also d'Haenens, Vandoninck, & Donoso, 2013). Adult reports are treated both as benchmarks and as having a higher truth value than those from children, as they are perceived as more «objective».[36] However, comparative research, where both children and parents have been asked about the children's practices, has shown how parents often do not have the correct understanding, knowledge or perception of the children's activities and experiences, also, and perhaps especially, when the questions asked are about risks (Staksrud, 2003; Staksrud, 2008).[37] Issues related to children and media typically creates policy interest. Media and children often triggers strong fears in parents and other adults: the end of innocence in our children, and the uncertainty of the new, unfamiliar media and its potential negative influences (Staksrud & Kirksæther, 2013). Thus, there is also a long tradition for questions about (new) media and children creating media panics.

36 For a more detailed account of such research models and their implications see Hogan (2005, pp. 24–26).

37 There are honourable exceptions to be noted of quantitative surveys in the field of children, Internet and online safety that have had children as informants. Most such surveys have taken place during the past decade, and many have been funded by the European Commission or by national governments (see Staksrud (2011, pp. 57–59) for a comprehensive list). Some of the research projects also included conducting interviews with parents, making comparisons between children's and parents' accounts of the same online experiences and practices. Such comparisons can be seen as a sign of valuing children as informants, making their voices at least as important as their parents.

Thomson (2007, p. 207) makes an interesting point about how within methodology and methodological research there is «a tendency to employ a meta-narrative of 'children' that is based in the polarized, fixed and separate identities of child and adult», questioning the myth of the all-powerful adult and the incompetent child. This information is then used to inform policy development and regulatory initiatives – also in the field of the Internet. Could it be that as we label something as «research with children», we might automatically set a confined frame of reference for our Internet-related research as well? Or, to put it another way: is the adult-child constellation something of a sociological dichotomy within research that should be more fully discussed as such (Staksrud, 2011, pp. 54–56)?[38]

The rationale behind such research approaches *with* children, as opposed to *on* them, is that children are viewed as agents in their own life and competent and capable of answering questionnaires and participating in research. There is also an underlying belief in and respect for their ability to answer questions about their own lives, experiences and feelings – on this they are the experts. Thus, I place myself alongside Saporiti (1994), arguing for seeing childhood as a status with the methodological consequences that follow, including utilizing age as a practical device for making distinctions, but not as the only criterion for assessing the status of children and childhood (Saporiti, 1994, p. 194). This is, however, a fairly new approach. Historically there is a long and crude tradition of research *on* children,[39] where asking them directly about issues concerning

38 For an overview of other various and typical sociological dichotomies and discussions thereof see Jenks (1998).

39 Most of the documentation of this approach can be found in the field of medicine. Using children (especially those institutionalized, such as in orphanages, with little protection from authorities) for medical experiments (of which exposure to viruses and the testing of vaccines would be a typical example) have been quite frequent, as the children often were «cheaper than calves» (Swedish physician of

them would not be considered a sound methodological approach. According to Borgers, de Leeuw & Hox (2000), the first direct account of how to interview children came in the 1954 edition of *The Handbook of Social Psychology* (Maccoby & Maccoby in Lindzey, 1954), but for the most part methodological accounts of research with children were based on ad-hoc knowledge from diverse fields.

At the same time there is a need to recognize that children may be vulnerable and in need of special attention and protection throughout the research process. Additionally, one needs to pay attention to other differences such as their physical size and strength compared to adults, their general social and legal status and their dependence on others and fixed institutional position (such as in schools) (Hill, 2005, pp. 62–64). Reflecting upon and adjusting to all these issues and processes are part of levelling the power-field, not between adult and child in particular, but rather between researcher and informant, as it is thought that in all research the researcher will come from a place of authority.[40]

With the above observations as background, I now turn to two practical examples of how one might make children count when researching online environments. Both are examples of cases in which the researchers' key aim was to make children count, taking a child-centred perspective in the collection of high-quality research data related to policy evaluation and development in the area of children and online safety and risk. The first example is about being open to children's voices without providing an adult frame

late 1800 quoted in Lederer & Grodin, 1994, p. 12). Thus, the history of pediatric experiments is largely a history of child abuse (Lederer & Grodin, 1994, p. 19). Also, within the social sciences there is a historical predominance of research on children as objects rather than with them as subjects, treating children as variables rather than persons (Greene & Hill, 2005, p. 1). (For accounts from the field of developmental psychology see Hogan (2005).

40 For a critical discussion on the various positions researchers can take in relation to children as informants see for instance Lahman (2008).

of reference and definition. The second example is about how we might make children count by researching from theirpoint of view.

Example 1: Listening to the child[41]

The first example relates to the following above-mentioned challenge: How can we make sure that we do not replicate standard perceptions of minors' Internet use, but rather open up the field to gain new insights? Representative, statistical surveys constitute one of the most efficient research tools in terms of applicability to policy development. Politicians as well as journalists appreciate the value of being able to say «how many» or «how much» in identifying or presenting a problem or an issue. Using statistics to frame current events might be particularly meaningful when the numbers represent a majority or a minority view, as this speaks to political language with its rhetoric and its need to frame standpoints in a prioritized context as «more» or «less» important than other issues on the agenda. Similarly, representative statistics can help define the appropriate, financially sound or «fair» limits for state-based services to groups of the population.

So, the legitimacy of policy development and intervention in Western societies partly relies on the ability to generalize findings to the population as a whole, or to specific, demographically defined sections of it. Statistical analysis is *especially* favoured within risk analysis, management and assessment studies, as statistics are helpful when relating to laypersons, such as politicians and the public. This is because one can contextualize any given risk by reliably comparing the likelihood of the risk happening with another type of risk, and by this aid the understanding of it by putting it in perspective. A strong argument can also be made that in regard to issues of risk, where the power of definition

41 This example, including the quotes, is taken from Livingstone, Kirwil, Ponte, & Staksrud (2013; 2014).

of perception, scope and management is often in the hands of «experts» (such as academics), statistics can *counter* predictable biases that also exist among experts – since experts are also people (Meadow & Sunstein, 2001).

When using (representative) surveys as a tool for mapping the state of the art and providing policy recommendations, one generally asks closed-ended questions about areas of already-established policy interest and agendas. One of the topics high on the agenda in relation to Internet policy is the question of online content regulation and what is perceived as harmful for children. Research on such questions can either be based on what is perceived as problematic by (adult) stakeholders in the field, or by researching what children actually do online and how their activities may or may not lead to distress and potential harm.

Although some qualitative research is beginning to investigate a wider array of possible risks to children online, much of the research is done within frameworks pre-defined by (adult) researchers. While such frameworks are firmly embedded both in theory, experience and observation, there is a need to ask if we miss out on the children's perspective. This is especially critical in the field of online research, with its fairly new and continuously shifting user patterns and rapid technological service innovations.

In order to counter this, when collecting data from a random stratified sample of 25,142 Internet-using European children aged 9–16 years (interviewing them at home during the spring and summer 2010), the children were first asked one open-ended, unprompted question: «What things on the Internet would bother people of about your age?' In recognition of the methodological and ethical challenges of researching children's conceptions of risk (Görzig, 2012; Ponte, Simões, & Jorge, 2013; Staksrud, 2013), each child was asked to write his or her answer privately on a piece of

paper and put it in a self-sealed envelope so neither interviewer nor parent (if present) could see how the child answered.

The results[42] (as reported in Livingstone et al., 2014) were as refreshing as they were surprising. First of all, the children expressed a considerable variety of risks that concern them on the Internet, for instance:

> The things that bother people about my age are the influence of bad websites such as how to diet or lose weight so you could be known as the pretty one; like vomiting things. (Girl, 15, Ireland)

> To take a photo of me without my knowledge and upload it to an inappropriate website. (Girl, 10, Bulgaria)

Yet, pornography (named by 22 % of children who mentioned risks) and conduct risk such as cyber-bullying (19 %) and violent content (18 %) were at the top of children's concerns online. Both surprising in its own right and a methodological reminder was the extensive priority given to violent content. This is noteworthy insofar as this area tends to receive less attention than sexual material or bullying in safety and awareness-raising initiatives and policy discussions. And, not only did a considerable group of the children mention violent content, they also elaborated on this as being realistic content from the news – typically accessed through

42 A standard coding scheme was used. Children's responses, written in 21 languages, were then coded by native speakers. One in three (38 %) identified one or more online risks that they think bothers people their age on the Internet (N=9,636 children: 5,033 girls and 4,603 boys). Response rates ranged from 73 % of children in Denmark to 4 % of those in Spain (with below 30 % also in Austria, Slovenia, Hungary, Bulgaria and Czech Republic). This variation may be due to genuine differences in children's level of concern, or it may have resulted from differences in fieldwork methodology. Of the 9,636 children who identified risks, 54 % identified one risk, 31 % identified two risks, and 15 % identified three or more risks. Up to three risks per child were coded, when applicable.

video-sharing sites such as YouTube. And many felt disgusted and scared:

> Some shocking news like terrorist attacks. (Boy, 12, Finland)
>
> I have seen what life was like in Chernobyl. People were suffering from physical deformities. I was upset to see the pictures and it made me sad. (Girl, 9, France)
>
> I was shocked seeing a starving African child who was going to die and a condor waiting to eat him. Also, news about soldiers who died while serving [in] the army, Palestine and Israel war scenes upset me very much. (Girl, 13, Turkey)

Thus, tweaking the methodology to let the digital users, in this case children, be heard gives direct and practical implications for future policy priorities. This procedure also connects online user research to traditional media user research both theoretically and empirically. In addition, it is a reminder of why and how children should be consulted also when the foundation is laid for policy development and solutions for protection are being sought (Livingstone et al., 2014).

So, an answer to our first challenge might be that in order to make sure we do not replicate standard perceptions, but open up our field to gain new insights, we need to actually ask the users – in this case children – themselves. Allowing them to freely reflect upon their own situations showed how policy and awareness work in the field of Internet safety was not on par with the actual worries of many children.

Example 2: Becoming the child

As stated in the introduction, researchers can and perhaps should have a key role in the evaluation of Internet self-regulatory initiatives. This second example therefore relates to the two challenges

of 1) How can we research communicative features and user practices in online communication services, such as social networking sites, without compromising the privacy and integrity of third party users? and 2) How can we as researchers fulfil our mission of independence and critical reflection on policy development in a field where businesses rather than governments are the principal regulators?

In 2008, as part of its Safer Internet Plus Programme, the European Commission gathered 18 of the major online social networks active in Europe as well as a number of researchers and child welfare organizations to form a European Social Networking Task Force to discuss guidelines for the use of social networking sites by children and young people (Staksrud & Lobe, 2010, p. 10). As a result, «The Safer Social Networking Principles for the EU» were developed as a self-regulatory scheme. The aim was to «provide good practice recommendations for the providers of social networking and other user interactive sites, to enhance the safety of children and young people using their services»[43] (European Commission, 2009), answering the challenge of providing regulation in a field where the single nation-state has limited capacity and options.

The guidelines were adopted voluntarily by the major online social networks active in Europe, and signed on Safer Internet Day,

43 Within the context of the principles, «social networking services» are defined as services that combine the following features (Arto et al., 2009: 3): a platform that promotes online social interaction between two or more persons for the purposes of friendship, meeting other persons, or information exchange; functionality that lets users create personal profile pages that contain information of their own choosing, such as the name or nickname of the user, photographs placed on the personal page by the user, other personal information about the user, and links to other personal pages on the service of friends or associates of the user that may be accessed by other users or visitors to the service; mechanisms to communicate with other users, such as a message board, electronic mail, or instant messenger; and tools that allow users to search for other users according to the profile information they choose to make available to other users.

February 10th, 2009.[44] The principles are meant as a guide for providers of social networking sites (SNS) providers when they seek to minimize potential harm to children and young people (Arto et al., 2009: 1). They recommend a wide range of good practice approaches, allowing for the diversity and internal judgment of the social networks themselves in terms of relevance and implementation. To honour their commitment the signatories regularly reported on their adherence to the rules and the implementation of information and technical tools that would make the use of social networking services safer for children.

As part of its extensive encouragement and support of the self-regulatory initiative of the SNS providers, the European Commission did commit to monitoring the implementation of the principles as part of its extensive encouragement and support of the self-regulatory initiative of the SNS providers by supporting independent researchers to assess the services. But how could this be done? The self-reporting from the services on their adherence to the principles would be the first place to look.[45] But can one accept self-evaluation at face value?

Another method could be to look at and investigate the respective social networking sites as a user, making sure that the described information and services were there and could be found. But would this guarantee a *safer* social networking site for *children*? And how could researchers, with their pledge to produce ethically sound and verifiable knowledge, contribute to this?

---

44 Please refer to the original report (Staksrud & Lobe, 2010) for more detailed information on the signatories and the relevant SNS services they offer.

45 Self-declaration reports were submitted by the social networks between April 10th and June 17th 2009. All these reports are public and can be downloaded from the European Commission's website: http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm#self_decl (link valid as of August 2009).

As many Internet researchers have learned, social networking sites are complex to review and research, as they usually contain and host a wide range of different (connected) services. This again makes them hosts of a range of (potential) online risks in terms of content, contact and conduct. This situation also raises a range of ethical issues, as the relational aspect means that you as a researcher, if you were to study children's (actual) use of the SNS by observing or engaging, would also study the communication and behaviour of *third parties* – other people the child is in contact with.

For instance: a commonly discussed problem high on the policy agenda related to children and media in general and to Internet services in particular is the potential for underage children to access inappropriate services. Many SNS's have age restrictions, e.g. Facebook has a 13-year-old age limit to sign up. If Facebook were to allow access by younger children, it would also have to comply with stricter rules of parental consent and handling of personal information as laid out in the US Children's Online Privacy Protection Act (COPPA) (United States Federal Trade Commission, 1998). According to the Safer Social Networking Principles, SNS's should ensure age verification mechanisms to prevent under-age users from signing up. However, when asking children about their SNS practices, researchers have found that a substantial number of under-aged users have profiles on these sites in general, and on Facebook in particular (Livingstone, Ólafsson, & Staksrud, 2013; Staksrud, Ólafsson, & Livingstone, 2013). What is the explanation for this state of affairs? Do children lie about their age? Or is it that the services are not sufficiently tailored to prevent unwanted users from signing up? In order to verify whether such preventive measures are in place, you would have to actually test the services in question. So why not use children? Would that not provide valid research results? Yes, but if «real», under-aged users were to be

used in the testing of the SNS features, either by observing underage children going online or by asking them to perform the equivalent of the test instead of adult experts, we would also knowingly have to:

- Ask them to do something illegal or in breach of terms of service and codes of conduct;
- Ask them to lie;
- Potentially expose them to new risks they might not be ready to cope with by making them sign up with services they have not previously used;
- Give the child an implicit or explicit acceptance of defined deviant behaviour;
- Teach children how to circumvent technical restrictions (and get away with it);
- Potentially ask children to do something they really do not want to do, but feel they must comply with;
- Potentially expose other underage children (third parties, e.g., «friends») as liars;

… to mention only some of the ethical challenges such a strategy would entail. In addition, of course, come the ethical dilemmas of ensuring informed consent from the child's parents or guardians as well as from the child him- or herself in order to do something that is illegal or at best a breach of the «terms of service» (but yet accepted practice by many parents, see Staksrud, Ólafsson, & Livingstone, (2013)).

The solution reached in this case was to develop a method that allowed for testing the SNS services from a child's perspective without the substantial ethical complications of involving actual children. Thus the researcher had to become the child.[46] This was

46 The author recognizes that the idea of «becoming» the child by setting up a social networking profile with a different persona carries with it problems and theoretical implications of its own.

done by developing a methodology[47] that directly tested the SNS features in question by using the often cited problem of social networking sites – you never know who is *really* on the other side of the profile or communication – to our advantage.

Addressing the ethical considerations relevant to testing such sites in the manner described, 13 carefully chosen national researchers were asked (while testing the sites) to choose imaginative nicknames/usernames for testing purposes and to set up a minimum of three profiles. In this way, the test avoided including any real underage children and the potential risks that such actions could have resulted in. Why three profiles? Because many of the features of SNSs extend from communication with other individuals. There is a need for «a friend» to communicate with, «like» and comment. The main testing profile was set up to be an 11-year old-girl (if possible, if not, a 15-year-old girl) with an «ordinary» name, all localized versions of «Maria». In addition, a peer-friend profile was established, as well as a profile of an adult. The latter was to be able to test whether adult «strangers» could access personal information about the minors, as well as if they would be able to contact them directly through the social networking site services.

The national experts were given detailed instructions on how to perform the testing in order to ensure as much consistency in the testing process as possible. The testing was meant to give a comprehensive and clear view of the extent of implementation of the principles in terms of compliance between what has been stated in the self-declarations *versus* how children experienced the sites in terms of online safety, help and information. It should also be

47 The test and methodology was been developed by the two lead experts Dr. Bojana Lobe, University of Ljubljana, Slovenia and Dr. Elisabeth Staksrud, University of Oslo, Norway. In the draft stage, the testing questionnaire was submitted to the Social Networking Task Force for comments and suggestions. The European Commission approved the final version. The test has later been used in subsequent testing initiated by the European Commission.

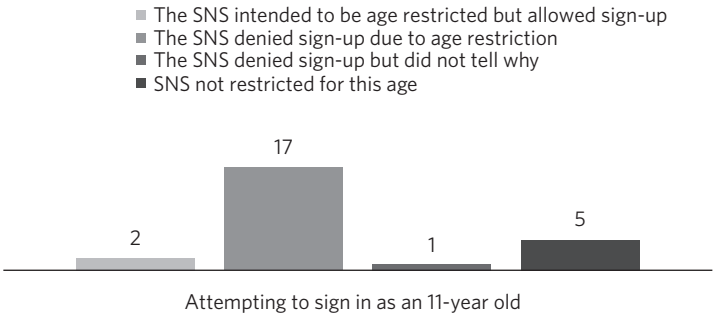

Figure 1 Attempts to sign up to age restricted sites

noted that all companies in question were told about the testing and evaluation in advance, and informed consent was ensured via the European Commission. The testers then tried to sign up for the service using the under-aged profile (Staksrud & Lobe, 2010, p. 26).

So, can 11-year-olds get access to a restricted site? When the results were collected it became clear that all services tested asked for information regarding date of birth as part of the registration process. On four services the users had to state that they were above a certain age (e.g. by ticking a box), while e-mail verification/address for e-mail verification was required by 20 services. Out of those 20 services, the testers were able to sign up without verifying over e-mail on seven of them.

On three services intended to be age-restricted for 11 year olds, sign-up was not allowed. 17 services denied sign-up, explicitly referring to the age restrictions on the site.

But children are people, and as people they might also employ strategies to circumvent restrictions. Thus it becomes important also to test if the services hold when children do something active to get access, such as changing their age.

Accordingly, for services that restricted signing up, another attempt was made *with the same profile*, but with the date of birth

of a 15-year-old girl. On seven services changing the date of birth/age was enough to grant access. On two additional services this could be done after a cookie was removed. *All* testers were later able to sign up *with a new profile* as an older user adhering to the age-requirements of the service on the same computer/device, regardless of previous failures.

Another example pertains to the principle of «Provide easy-to-use mechanisms to report conduct or content that violates the terms of service» for children (principle no.4 of the SNS self-regulation agreement). This was specified as:

- Providers should provide a mechanism for reporting inappropriate content, contact or behaviour as outlined in their Terms of Service, acceptable use policy and/or community guidelines. These mechanisms should be easily accessible to users at all times and the procedure should be easily understandable and age-appropriate.
- Reports should be acknowledged and acted upon expeditiously.
- Users should be provided with the information they need to make an effective report and, where appropriate, an indication of how reports are typically handled. (Arto et al., 2009, p. 8)

In order to test principle 4, the social networking sites were sent the following message from the expert testers on their service(s) if at all possible.[48]

> «I am writing to you because someone is sending me scary messages. What should I do about this? Please help me.»

This message was carefully designed and worded to be a general request, and would in most cases be sent from the profile of a

48 On a few services it was not possible to send a general request asking for help, but rather requests pre-defined by the SNS. In these cases the tester was asked to send the pre-defined report that resembled the original message the most.

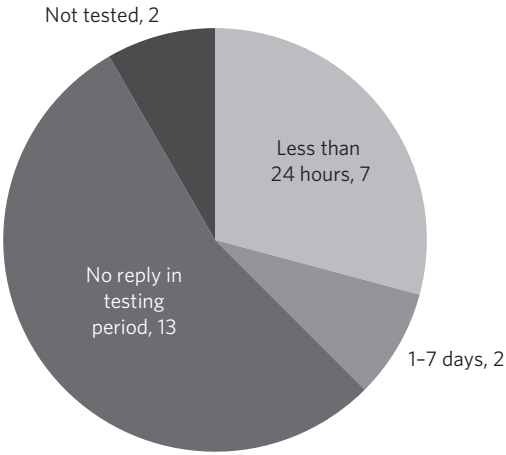

Figure 2 Response time to users of Social Networking Services when asking for help[49]

registered, underage user of the site (in most cases an 11-year-old, in a few cases a 15-year-old, depending on the overall age restriction of the SNS). In this message, the SNSs were asked to give specific advice on how the users themselves should handle the situation. Please note that the message did not mention the SNS in particular. It was a general cry for help.

As the signatories are very diverse in the services they provide, this message might not be fully relevant to all the 20 social networking sites that at that time committed to the principles. However, it was deemed that an underage user asking for advice and help from a professional party should receive some sort of feedback, preferably with information relevant to the request sent. The way the message was worded should also prompt a personal response. So, did they get one?

Figure 2 gives an overview of the response time of the SNSs. Only relevant feedback was listed as a response, hence automatic

49 Figure adapted from Staksrud & Lobe (2010, p. 33).

responses only stating that the message has been received and will be reviewed are not deemed sufficient to be listed as a full «reply».

Of a total of 22 services tested, 13 did not give any reply to the message asking for help during the testing period of about 6 weeks, two replied within a week (3–4 days), while seven replied within 24 hours.

From a policy point of view, the results were discouraging and signalled a failure to commit to the practical implementation of the SNS principles. As such it serves as a reminder that in terms of policy, including those implemented to protect user rights and safety, there is a distinct difference between the stated state of the art and the reality as experienced by the user.

From a research and methodological point of view, however, the undertaking was a success, in that it ensured quality data without compromising the integrity of the users.

One answer to challenge no. 2, then, «How can we research communicative features and user practices on online communication services, such as social networking sites, without compromising the privacy and integrity of third party user?», is that we sometimes need to go undercover. As observational research on the use of social networking services inevitably will involve not just one informant, it is vital that third parties also are protected according to ethical standards. This is especially critical as you might never really know who is on the other side of the interaction. Your primary informant might be interacting with a minor.

This example is also a reminder that if we as researchers are to fulfil our mission of independence and critical reflection on policy development in a field where businesses rather than governments are the principal regulators (challenge no.3), we need to take a critical approach and avoid relying on self-reporting as the (only) tool of assessment. The example also highlights the need for in-depth, real-world use and testing. This is particularly important with services offered in several countries and languages, where the

risk of differences between «versions» is present. It is the end-user experience that should be evaluated, not their guardians' report on it, nor the service provider's own account of their system and routines. When said out loud this seems self-evident, but the history of research on children's use of online digital media says differently.

Conclusion

Unlike other places in life, where the mismatch between parental perception and children's activities can often be observed, not only by researchers, but by the individual citizen, the online lives of children and the features of the digital services they use slip beneath most people's radars. It is the researcher's trade and obligation to provide critical, quality research to inform policy. In the online field our job might be harder, but no less important. However, we might take some comfort in the fact that new technologies do not necessarily mean new methodologies, simply new approaches.

References

Arto, bebo, Dailymotion, Facebook, Giovani, Google, … wer-kennt-wen. de. (2009). Safer Social Networking Principles of the EU. Luxembourg: European Commission.

Borgers, de Leeuw, & Hox. (2000). Children as Respondents in Survey Research: Cognitive Development and Response Quality 1. *Bulletin de Méthodologie Sociologique, 66*(1), 60–75. doi: 10.1177/075910630006600106

Bruhn Jensen. (2002). The social origins and uses of media and communication research. In K. Bruhn Jensen (Ed.), *Handbook of media and communications research: qualitative and quantitative methodologies* (pp. 273–293). London: Routledge.

Children's Online Privacy Protection Act of 1998, Title 15 C.F.R. § 6501 (1998).

d'Haenens, Vandoninck, & Donoso. (2013). How to cope and build online resilience? *EU Kids Online*, http://eprints.lse.ac.uk/48115/1/How%20to%20cope%20and%20build%20online%20resilience%20%28lsero%29.pdf: London School of Economics and Political Science.

David, Tonkin, Powell, & Anderson. (2005). Ethical aspects of power in research with children. In A. Farrell (Ed.), *Ethical research with children* (pp. 124–137). Maidenhead, England: Open University Press.

European Commission. (2009). Safer social networking: the choice of self-regulation Retrieved 20.08.09, 2009, from http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm#self_decl

Farrell. (2005). *Ethical research with children*. Maidenhead, England: Open University Press.

Görzig. (2012). Methodological framework: The EU Kids Online project. In S. Livingstone, L. Haddon & A. Görzig (Eds.), *Children, risk and safety online: Research and policy challenges in comparative perspective* (pp. 15–32). Bristol: Policy Press.

Greene, & Hill. (2005). Researching children's experience: methods and methodological issues. In S. Greene & D. Hogan (Eds.), *Researching Children's Experience. Methods and Approaches* (pp. 1–21). London: Sage.

Hill. (2005). Ethical considerations in researching children's experiences. In S. Greene & D. Hogan (Eds.), *Researching Children's Experience. Methods and Approaches* (pp. 61–86). London: Sage.

Hogan. (2005). Researching 'the child' in developmental psychology. In S. Greene & D. Hogan (Eds.), *Researching Children's Experience. Methods and Approaches* (pp. 22–41). London: Sage.

Jenks. (1998). *Core sociological dichotomies*. London: Sage.

Lahman. (2008). Always Othered. *Journal of Early Childhood Research, 6*(3), 281–300. doi: 10.1177/1476718x08094451

Lederer, & Grodin. (1994). Historical Overview: Pediatric Experimentation. In M.A. Grodin & L.H. Glantz (Eds.), *Children as research subjects: science, ethics, and law* (pp. 3–25). New York: Oxford University Press.

Lindzey. (1954). *Handbook of social psychology*. Reading, Mass.: Addison-Wesley.

Livingstone. (2003). Children's use of the Internet: reflections on the emerging research agenda. *New Media Society 5*(2), 147–166.

Livingstone, Kirwil, Ponte, & Staksrud. (2013). In their own words: What bothers children online? *EU Kids Online III* (pp. 20): London School of Economics and Political Science.

Livingstone, Kirwil, Ponte, & Staksrud. (2014). In their own words: What bothers children online? *European Journal of Communication, 29*(3), 271–288. doi: 10.1177/0267323114521045

Livingstone, Ólafsson, & Staksrud. (2013). Risky Social Networking Practices Among «Underage» Users: Lessons for Evidence-Based Policy. *Journal of Computer-Mediated Communication, 18*, 303–320. doi: 10.1111/jcc4.12012

Meadow, & Sunstein. (2001). Statistics, not experts. *Duke Law Journal, 51*, 629–646.

Ponte, Simões, & Jorge. (2013). Do questions matter on children's answers about internet risk and safety? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 7*(1). doi: 10.5817/cp2013-1-2

Saporiti. (1994). A Methodology for Making Children Count. In J. Qvortrup, M. Bardy, G.B. Sgritta & H. Wintersberger (Eds.), *Childhood matters: social theory, practice and policies* (pp. 189–210). Aldershot: Avebury.

Staksrud. (2003). *What do SAFT kids do online*? Paper presented at the Future Kids online – How to Provide Safety, Awareness, Facts and Tools, Stockholm, Sweden.

Staksrud. (2008). Fairytale parenting. Contextual factors influencing children's online self-representation. In K. Lundby (Ed.), *Digital Storytelling, Mediatized Stories: Self-representations in New Media* (pp. 233–249). New York: Peter Lang.

Staksrud. (2011). *Children and the Internet: Risk, Regulation, Rights*. PhD PhD, University of Oslo, Oslo.

Staksrud. (2013). *Children in the Online World: Risk, Regulation and Rights*. Surrey: Ashgate.

Staksrud, & Kirksæther. (2013). 'He who buries the little girl wins!' – Moral panics as double jeopardy. The Case of *Rule of Rose*. In J. Petley, C. Critcher, J. Hughes & A. Rohloff (Eds.), *Moral Panics in the Contemporary World* (pp. 145–167). London: Bloomsbury Academic.

Staksrud, & Livingstone. (2009). Children and online risk: Powerless victims or resourceful participants? *Information, Communication & Society, 12*(3), 364–387. doi: 10.1080/13691180802635455

Staksrud, & Lobe. (2010). Evaluation of the Implementation of the Safer Social Networking Principles for the EU Part I: General Report. Luxembourg: European Commission under the Safer Internet Programme.

Staksrud, Ólafsson, & Livingstone. (2013). Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior, 29*(1), 40–50. doi: http://dx.doi.org/10.1016/j.chb.2012.05.026

Thomson. (2007). Are Methodologies *for* Children keeping *them* in their Place? *Children's Geographies, 5*(3), 207–218. doi: 10.1080/14733280701445762

Social research and Big Data – the tension between opportunities and realities

Kari Steen-Johnsen and Bernard Enjolras
Institute for Social Research
kari.steen-johnsen@samfunnsforskning.no
bernard.enjolras@samfunnsforskning.no

In a passionate argument for the idea that social research must adopt social transactional data generated through new information technologies and new analytical techniques, Savage and Burrows claim that:

> both the sample survey and the in-depth interview are increasingly dated research methods, which are unlikely to provide a robust base for the jurisdiction of empirical sociologists in coming decades. (Savage and Burrows, 2007: 885)

Savage and Burrows base their claim on the argument that digital data on social transactions is data about actual events, while also being data that pertains to entire populations. While the survey depends on representative samples and makes predictions based on such samples, those who analyze web data have direct access to complete data about actions and statements. In other words,

analysts of digital transactional data, or what has frequently been termed «Big Data», evade the problem of representativeness: they can provide actual descriptions of peoples' actions and infer future actions from these. This has proven a strong tool for predictions, as exemplified by how Amazon.com is able to make book recommendations to customers based on the choices made by thousands of other customers. In a situation where response rates are falling, data from social transactions provides a powerful alternative. The argument against the qualitative in-depth interview is that this method is incapable of grasping the complexity that modern life entails. According to Savage and Burrows, this complexity can be better grasped in its entirety by studying large numbers of cultural expressions – pictures, videos and texts on the Internet.

There is no doubt that the use of Big Data in research presents researchers with new opportunities for analyzing social phenomena. Yet the use of such data also has its limitations, and introduces a set of new ethical and practical challenges. Both the opportunities and challenges are not only closely linked to the very nature of data, but also to how ownership and access to data are regulated.

In this article, we will attempt to shed light on the role of research in a field of tension between the new opportunities data offers, the ethical considerations that are necessary when a person carries out research and the limitations that exist in the regulation of and access to digital data. Underlying our considerations is the realization that the way in which we as researchers approach this field of tension has consequences. When we study social transactions through Big Data, we are studying a social reality. Through research, we participate in both constructing a social reality, such as the digital public sphere, and giving society insight into what its social reality is, both of which can have social consequences.

First, we want to describe what characterizes digital transactional data and what kinds of opportunities it offers to research. We will

use the term Big Data in order to underscore the new analytical opportunities embedded in the characteristics of digital data, and use social media data as our main case. Then we wish to say something about the new ecosystem that has emerged around the production, gathering and analysis of digital data, and how it changes the research premises for the production of knowledge. We have borrowed the idea that the use of Internet data must be understood as being a part of the growth of a new ecosystem from boyd & Crawford's article «Critical Questions for Big Data» (2012). By using the term *ecosystem*, we emphasize the idea that it is important to understand the use of such data in a context, where various formal and informal actors position themselves, compete and influence each other in the production and use of Internet data. At the end of this article, we will discuss the role of research, both in relation to representing the social reality that is created by digitalization, and in relation to the fact that research itself is an actor with a place in a new ecosystem that is linked to the production of knowledge.

Big Data – what is it and what can it be used for?

The amount of available digital data about people has exploded in recent years. This has to do with mundane status updates on Facebook, videos posted on YouTube, and Twitter posts that are available to anyone who wants to read them. It also pertains to data from purchases, both those that are made on the Internet and those that are made by credit card. Other examples of digital data include data from Google searches and data that logs phone calls.

The term «Big Data» is a collective term for data that is of such a scope that more data power than normal is required in order to collect and analyze it (Manovich, 2011). The term is often used not only to simply describe the data itself, but also to describe the new

technical, legal and ethical issues such data gives rise to. Big Data are regularly collected in a number of areas, related to natural, technical or social phenomena. For present purposes we understand Big Data to be data containing person-related information. What phenomena characterized in terms of Big Data thus understood have in common with each other is that they involve a registration of actual events, interactions and transactions connected to individuals.

There are two aspects of Big Data in particular that will greatly impact the social sciences. First, transaction data differs from survey data in that such data directly reflect what individuals actually do, instead of drawing conclusions based on individuals' statements about actions. Second, digitalized data combined with cheap data power make it possible to study entire populations, instead of drawing on a selection. Thus, it becomes possible to conduct very sophisticated analyses, and also to predict future actions. In the book *Predictive analytics. The power to predict who will click, buy, lie or die* (2013), Siegel provides examples of such predictions within several areas: within the banking system, in the struggle against crime, and in health-related services. One example that pertains to many people's daily lives is the way in which companies such as Amazon.com are using previous purchase data to market and offer relevant products to the individual user: «Other people who bought this book, also bought …». One example from the field of health is how Google was able to use search trends to predict the development of the swine flu epidemic long before the national health institutes could do so.

The way in which Obama's second presidential campaign used and analyzed data provides examples of both how data may be used to predict behaviour, and how data from different sources can be pulled together and offer powerful analyses.[50] Obama set

50 See http://www.technologyreview.com/featuredstory/508836/how-obama-used-big-data-to-rally-voters-part-1/ for a thorough description of how the Obama campaign worked with Big Data and predictions.

up a separate computer lab that linked data regarding households, previous voter behaviour, previous donations and television use, and then tailored his message to individual voters based on such data. This afforded him the ability to choose where to direct his efforts – and with which message – in a much more efficient manner than would otherwise have been possible using traditional analysis and prediction methods.

The example of Obama highlights an important characteristic of digital transactional data, namely that such data contains several layers of information. Metadata, such as email addresses, make it possible to link the different data that an individual has produced, for example data about purchase transactions and toll transactions. Savage and Burrows (2007) emphasize the importance of the fact that digital transactional data contains information about one's geographical positioning, and claim that many of the classic background variables in sociology can collapse into one variable as a basis for predicting actions. In this argument they rely on a set of studies that have demonstrated that neighbourhood location is a more significant predictor of many outcomes than other person or household-related variables (2007: 892). The possibility of determining one's position grows with the increased use of handheld media devices. In addition, different types of data from various sources are linked together and integrated through social media and the different Internet sites where individuals have user accounts. For example, Facebook integrates several different applications, such as Spotify, Instagram, and Farmville, and the data about activity on the different applications are thereby linked together. A parallel example is the link between Google, Gmail, YouTube, Chrome and Google+.

The result of this linking of data is that it creates new opportunities for assembling very detailed information, not only about individuals, but also about groups and organizations. One characteristic of the

built-in opportunities for action in social media is that they make it possible to establish a social graph – lists of followers and friends (boyd & Ellison, 2011). Data gathered from social media thus contain information about how individuals and groups are linked together. If data about a user is collected on Facebook, data is simultaneously collected about several people in this user's network.

Opportunities and limitations for social research

It would appear that such data represent an obvious enrichment to social research, as they give direct access to people's lives, statements and actions, provide detailed information and can be easily collected. Both access to Internet data and the opportunity to conduct analyses of large datasets based on concrete actions and interactions have caused many researchers to feel that the use of Internet data will revolutionize social research in fundamental ways.

However, in the article «Critical Questions for Big Data», boyd and Crawford caution against believing we can leapfrog over fundamental methodological challenges, such as the issue pertaining to representativeness, when the data that is used is large enough. Analyses of Twitter provide a good example of some of these challenges. Twitter studies have become very popular internationally, especially due to the availability of data. However, questions may be raised as to what analyses of Twitter posts represent. An obvious challenge is that Twitter users only constitute a certain selection of the population. Other issues are linked to the fact that there is no one-to-one-relationship between user accounts and actual people. One person can have several accounts, several people can use the same account, and accounts can also be automated – so-called «bots».

Another problem is linked to the definition of what constitutes an active – and thereby relevant – user on Twitter. According to Twitter, as many as 40 per cent of their users in 2011 were so-called «lurkers», that is, users who read content without posting anything themselves. Brandtzæg showed in his doctoral thesis that the same finding pertained to 29 per cent of those who use Facebook in Norway (Brandtzæg, 2012). The question then is how to get hold of and define a representative picture of social media as both forums for distributing information and as «public spheres». One response to this might be to argue that the use of Big Data makes it possible to analyze social media sites like Twitter or Facebook on an aggregate rather than an individual level, and in this way paint a picture of these social media as public spheres based on whatever and wherever topics are being discussed and distributed.

Another example of the difficulties in determining what constitutes the correct representation of the digital public sphere may be found in our contribution to Enjolras, Karlsen, Steen-Johnsen & Wollebæk (2013). In this book, one of our aims is to study public debate as it takes place in social media. The basis for the book is a web-based, population representative survey that we repeated on two occasions, where we posed fairly detailed questions about where people debate, what kinds of topics they discuss, and how they experience the debate (for example, whether they often debate with people who agree with them).

Based on analyses of the material, we paint a picture of a fairly well-functioning public debate: the debating Internet population is hardly distinct from the population in general when it comes to socio-economic background and political views. Many debate with people they disagree with, few experience getting hurt, and many learn something from the experience – though few change their opinions. We also draw a comparison of political attitudes among

those who debate on the Internet and those who do not, a comparison which is broken down into different forums (Facebook, discussion forums, Internet papers, blogs, etc.). As a whole, there are hardly any differences between those who engage in discussion on the Internet and those who do not. There are differences, however, between debaters on the various platforms. This picture differs significantly from the picture that is sometimes presented in the mass media and the socially mediated public sphere. At the same time, there is little doubt that if we conducted a thorough qualitative examination of the content from selected discussion forums and the debate forums of online newspapers, and studied the political attitudes within them, we would find a different picture. These two approaches would both give valid representations of Internet online discussions, but they would be representative of different phenomena – either the broad picture or the dynamics of particular forums.

This example illustrates the argument that, depending on whether one uses selected web content or representative survey data as the basis for analysis, very different pictures of an Internet phenomenon can be obtained. The same phenomenon is pointed out by Hirzalla et al. (2011) who point out that in studies about whether the Internet equalizes differences between different groups when it comes to political participation, it is often the case that those who conduct case-based research are more optimistic than those who conduct survey research when it comes to their mobilizing potential. Those who study the Obama campaign's social networking sites will most likely find a stronger source for the mobilizing power than those who study the American population's activism through survey-based methods. The representative picture and the picture that is based on significant events thus part ways – but which picture is the most valid in relation to how the digital public sphere works?

Even though the use of Internet data may potentially provide access to complete data and enable researchers to analyze statements and content from a large number of users, this does not eliminate the problem linked to representativeness or the need to interpret and discuss whatever phenomenon a person has captured. In addition, it is important to point out that the assumption of having complete data is hardly ever correct. We can again use Twitter as an example. Only Twitter has complete access to the information in Twitter accounts and the complete set of Twitter posts. Twitter makes Twitter posts available through so-called APIs,[51] which are program sequences that make it possible for outsiders to retrieve Twitter posts. However, it is unclear what underlying factors are at work in such retrievals, for example, on what grounds the selection is made. The selection of Twitter messages can also become uneven due to the fact that Twitter censors certain types of unwanted content.

What characterizes the new ecosystem for the production of knowledge?

In connection with the increased access to digital data, important changes have taken place in the social landscape where research positions itself. Savage and Burrows use the term «knowing capitalism» to describe a new social order in which social «transaction data» become increasingly important, and where such data are routinely collected and analyzed by a large number of private and public institutions. The main point for Savage and Burrows is that research has thereby ended up in a competitive setting. Research is no longer the dominant party when it comes to providing interpretations of society. boyd and Crawford use the concept

51 API stands for «application programming interface» and is a software that can be used to collect structured data, for example from Twitter (boyd & Crawford, 2011: 7).

of a new «ecosystem» to describe the new set of actors connected to the analysis of digital data and the power relationship that exists between them. Several elements of this new ecosystem touch on the potential of social research to represent and interpret society. We will highlight a few of these elements here.

First, the ownership of data has become privatized. While access to data has traditionally depended on an exchange between researchers and individuals who have given their consent, such access now largely goes through large, private companies such as Google, Twitter, and Facebook. Also, several other types of commercial businesses, such as telecommunication companies, banks and online bookstores, are in possession of large amounts of data. This situation creates several challenges for research. The fact that data are owned by private actors makes the access to such data and assessments of the quality of data difficult. Further, a gap arises between these private actors and externally performed research, because the owners of the data have access to complete sets of data. Several of the large Internet actors, such as Facebook and Google, have their own research departments with a high level of competency that enjoy the benefits of having complete access to the data.

As the data are under private ownership, these research departments are not in the same situation when it comes to privacy protection as researchers are, for example when it comes to requirements regarding informed consent. This is because users are required to accept the terms and conditions for the use of their digital data in order to be able to use the service. The result is that actors outside of academic research get a jumpstart when it comes to providing relevant social analyses and interpretations. Besides the fact that researchers inside these private companies are in a position to produce unique analyses, it is a problem that they are not required to let their research be reproduced or evaluated through the examination of data, given the fact that the data are private property

(Enjolras, 2014). Moreover, there is no requirement to let results be examined critically by the international researcher community. In the long run this may lead to a privatization of social research.

Second, the access to new types of data leads to research activity being disconnected from traditional research institutions, which again leads to a situation where «everyone can conduct research». Despite the tendency towards privatization, it is still a fact that a great deal of data is available to the general public on the Internet. A consequence of this is that a much greater number of people can now conduct some form of research or investigations. One trend is that there is a growth in payment services that allow people and organizations to analyze Internet data linked to their own business and to conduct surveys via the Internet. An important example is Google Analytics, which offers tools for analyzing the Internet activity linked to various companies or organizations. The interpretations derived from the research of digital information thus compete with several other narratives coming from individuals, organizations, and analyst agencies. These are not necessarily based on observations of the data's representativeness and quality or on a suitable theoretical foundation.

Third, the development leads to powerlessness among the average Internet user. While digitalization offers new opportunities to many people for gathering information, expressing opinions and analyzing digital data, the users' control over their own data is being reduced. The privatization described above is an important reason for this. To be able to use popular services such as Facebook and Twitter, we have to give these applications access both to basic data and to utilizing these data for their purposes. Such use can consist of generating analyses and statistics, resale efforts and marketing purposes. It can be difficult for the user to understand what rights she or he is really giving up.

As described above, a complicating element is the complexity of digital data. The fact that data exist in many layers, with different

kinds of information, constitutes one such complexity. The fact that different data gathered from different applications and websites are linked together is another. In addition, it is hard to get a full overview of what the network structure in data really entails. For example, those who gather information about you can also at the same time gather information about the users in your network, and vice versa.

The difficulties in understanding both the technical and legal stipulations for the use of an application mean that users lose control over their own statements. A survey conducted in 2009 by Brandtzæg and Lüders in regard to Internet use and privacy protection revealed that many users were concerned about the consequences of sharing personal information on the Internet. The study also showed that most users had limited insight into how social media function and how to handle the privacy settings. boyd & Crawford call attention to the fact that data that have been produced in a certain context may not necessarily be brought into another context just because it is available (2012: 672). The conditions we have outlined here make it important for researchers to take this cautioning seriously. The users produce content within vague frameworks, and do not necessarily have full oversight over what data about them is available, and what it can be used for.

New digital dividing lines

Based on the preconditions that exist in the new ecosystem linked to digital data, it is possible to see the contours of a set of digital dividing lines that will affect what knowledge is being produced by whom (boyd & Crawford, 2012: 674). We claim that academic social research is in danger of losing out in the battle of having access to producing knowledge based on these new types of data. Social research, or at least parts of it, is currently in a disadvantageous

position when it comes to certain disparity structures that will potentially strengthen over time.

An important disparity pertains to access to data and to the resources required to utilize them. As pointed out above, private companies and their analysis departments have privileged access to data. For those who wish to conduct research on such data, access is restricted, and financial resources are required. Digital data from different platforms have been commercialized and can be purchased through so-called «data brokers». Access is thus dependent on the financial resources one has available. Alternatively, one can also collect certain types of data, such as Twitter data, by programming APIs oneself, that is, programs that can fetch data based on certain criteria. However, this also requires resources in the form of data power. As a result of the requirements regarding finances and technological investment, a disparity emerges, not only between private actors and academic institutions, but also between the academic institutions. Elite universities, such as Harvard, MIT and Stanford, have resources to build and equip research environments with technology and resources that allow them to utilize digital data. Smaller universities may not have the same resources. In Norway, we can imagine dividing lines among both the universities and between the university sector and the research institutes.

The use of digital data also creates dividing lines when it comes to competency. In order to utilize such data, competencies in programming, analysis and visualization are required. Such competencies are still a limited resource within the social sciences and the humanities. Building up such competencies requires resources, and larger institutions have an advantage if they are able to connect technical and interpretative environments.

An important disparity-generating dimension has to do with the regulations and requirements that pertain to the use of Internet data. Here we can find several dividing lines. First, there is a

difference between different countries' legislation with regard to privacy protection connected to research on digital data when it comes to collection, information and storage. This creates differences when it comes to getting access to using such data. At present, there are efforts at the European level to harmonize regulations relating to data protection rules, among them regulations pertaining to research.[52]

Second, there is a fundamental gap between those who own digital data and those who do not. When consumers make use of services, such as mobile phones, bank cards or online shopping, or use Facebook or Google, they also give the providers of these services permission to use the personal data they enter by accepting the terms of conditions for the service. This permission allows private companies to stand in a privileged position when it comes to utilizing data, both for research and analytical purposes, as well as for commercial purposes, without having to abide by the same set of ethical guidelines that research does. The companies are not subjected to any requirements to make these data publicly accessible so that other researchers can make use of them.

It is not only reasonable but of some importance that research on digital data are subject to strict ethical requirements, especially considering the users' potential powerlessness when it comes to protecting their own data. At the same time, it can be claimed that current regulation posits some conditions that are not up to speed with the general public's perception of the boundary between public and private information, and the perception of what kind of information should be covered by the privacy clause. One example that was published in *Forskningsetikk* (Research Ethics) 1/2013 has to do with the use of Twitter posts in an aggregated form, for example if one wishes to analyze all Twitter posts

52 Cf. http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

with the hashtag #bevarhardanger (savehardanger). In relation to research based on such Twitter data, Kim Ellertsen, director of the Law Department at the Norwegian Data Protection Authority, emphasized the importance of informing Twitter users about the research. He also questioned the practical difficulties in reaching the users (Forskningsetikk 1/2013: 8). As pointed out by Ellertsen, the issue of the need to inform research subjects raises questions about whether the results are of general public interest and about the effects on freedom of speech. In our view, one key issue is whether these posts should be viewed as public statements on par with statements in newspapers and edited media or as personal information.

Referring to Manovich (2011), it is possible to claim that «the computational turn» has created a new hierarchy between those who produce data (that is, consciously or unconsciously leave data behind), those who have the tools to gather data and those who have the expertise to analyze them. boyd & Crawford point out that the latter group is the smallest and the most privileged, and it is the group that will have the most influence on how Big Data will be used and developed (2011: 113). There is a danger that large segments of social science research will be unable to contribute to these analyses.

The responsibilities and challenges of research

Internet research does not only present us with a new set of data and methods with corresponding ethical problems, but also with a new ecosystem for the production of knowledge. To define what the responsibilities of research are, we believe it is important to be aware of the fact that research plays a role in at least two different ways: as a producer of knowledge and as an actor with a shared

responsibility to develop and practise a code of conduct adapted to Big Data. Both of these roles are to some extent dependent on conditions outside the research itself, such as the activities of other actors and public and private regulations.

The role of research is thus primarily about providing knowledge about the new way in which information is stored and structured in a digital society, as well as to shed light on what kind of power different types of actors, such as citizens, elites, organizations, and states, possess when it comes to having access to and the ability to interpret information. This means contributing with research-based interpretations of what the Internet is and how it works. Researchers should take it upon themselves to provide understandings of both the structural qualities of the web and the social practices that develop within different social fields and among different groups. A major challenge for segments of the social sciences is addressing the methodological opportunities that the Internet and Big Data present us with in such a way that researchers will be able to provide these types of analyses. This requires an investment in a new competency which is not included in most of the researchers' basic education. A further requirement is a reflection on the methodological challenges and problems, such as the question of whom and what the different forms of web data represent. Through research, we take part in constructing the new information society as an object and providing the society with insight into what this reality is. This implies providing perspectives on such questions as: Do we understand the Internet as being open and free, or as something that is regulated and conditional? Does the Internet really constitute a public sphere, or rather a network consisting of isolated islands? Which voices are being represented in our research? What social interpretation is being produced that will potentially impact what legitimacy and significance the Internet will have in social political processes? Depending on which instruments,

methods and theoretical tools we, as researchers, use to attack the digital research field, we will be able to provide different answers to these questions.

The second role of research is about contributing toward developing an ethic that is adapted to the new premises laid out by digital systems and Big Data. We feel that such an ethic cannot be developed in a vacuum, but must take into account the ecosystem of knowledge of which research is part. The challenge of research is to produce valid research in an ecosystem of knowledge while being under pressure by privatization and ethical regulations that differ from one country to another, and which to varying degrees are adapted to digital data. One way to think about this is through the concept *accountability*, which can be understood as more encompassing than the concept of privacy protection (boyd & Crawford, 2011). Accountability is not only directed towards the research subject, but also towards the research field in a broader sense. Accountability implies reflecting on the consequences of research related to individuals, organizations and the public sphere, or towards potential shifts in the ecosystem regarding the production, collection and analysis of digital data. If independent researchers could get the same access to using and connecting private data that Facebook has, a researcher would perhaps not choose to summarily use them to analyze statements about, for example, religion and sexuality. The researcher must weigh her interest in providing solid, academic knowledge about a social phenomenon, against people's perceptions of digital forums, and their faith in them. If researchers choose to use material that is perceived as private or as taken out of context, this might violate both the legitimacy of social media and the legitimacy of research. At the same time, *not* using these data means that the researcher leaves it to Facebook's analytical department to interpret them. Such considerations must be carried out specifically in relation to different kinds of data and

linking of data, different kinds of subjects and the public's perception of these data.

Presenting interpretations of society is nothing new in social research, nor is the fact that these interpretations may have social consequences. Still, our claim is that the Internet presents us with a new set of challenges. It requires that we both understand and critically evaluate what kind of data Internet data is and what it can produce knowledge about, and that we understand the social context of this type of research The ethical dilemmas that Internet research presents cannot be resolved without a deeper reflection on and establishment of ground rules for how Big Data should be handled in society, where research and other forms of public and commercial data use are put into context.

The rules that pertain to digital data are adapted to a «small data» world, where both data and computing power are accessible in large quantities. The ethical challenges pertain not only to research, but also to industry and administration. Therefore, we need new forms of accountability for both research and society.

References

boyd, d. & Crawford, K. (2012). Critical Questions for Big Data. Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*. Volume 15, issue 5. pp. 662–679.

boyd, D. & Ellison, N.B. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication. Volume 13, Issue 1, pages 210–230.

Brandtzæg, P. (2012). Sosial Networking Sites: Their Users and Social Implications- A Longitudinal Study. Journal of Computer-Mediated Communication. Volume 17, Issue 4, pages 467–488.

Brandtzæg, P. & Lüders, M. (2009). Privat 2.0: Person- og forbrukervern i den nye Medievirkeligheten. SINTEF-Rapport.

Enjolras, B. (2014). Big data og samfunnsforskning: Nye muligheter og etiske utfordringer. *Tidsskrift for samfunnsforskning*, 55 (1). p. 80–89.

Enjolras, B., Karlsen, R., Steen-Johnsen, K. & Wollebæk, D. (2013). *Liker, liker ikke. Sosiale medier, samfunnsengasjement og offentlighet*. Oslo: Cappelen Damm.

Hirzalla, F., van Zoonen, L. & de Ridder, J. (2011). Internet use and political participation: Reflections on the mobilization/normalization controversy. Information Society, 27(1): 1–15.

Manovich, L. (2011). Trending: the Promises and Challenges of Big Social Data. http://lab.softwarestudies.com/2008/09/cultural-analytics.html#uds-search-results, retrieved 09-01.13.

Savage, M. & Burrows, R. (2007). The coming crisis of empirical sociology. *Sociology*. Vol. 41, no. 5. 885–899.

Siegel, E. (2013). *Predictive Analytics. The Power to Predict who will Click, Buy, Lie or Die*. Hoboken, NJ: John Wiley & Sons.

Studying Big Data – ethical and methodological considerations

Anders Olof Larsson

Department of Media and Communication,
University of Oslo

a.o.larsson@media.uio.no

Introduction

New technologies for communication tend to raise certain expectations regarding the more or less overwhelming societal influence arising from them. Such was the case with radio and television – and consequently, also during the mid-1990s, when the Internet started to grow in popularity throughout much of the Western world. While more traditional or established forms of media remain a major part in our everyday media diets, the Internet has indeed come to play an important role in our day-to-day activities. Needless to say, such a move to a variety of online environments is of significant interest to a variety of scholars from the social sciences and the humanities. This chapter presents an overview of some of the challenges of performing research on the activities taking place in such environments. While my personal experience with this type of research is geared more towards perspectives often

associated with the social sciences – specifically various aspects of online political communication – it is my hope that the concerns raised will also resonate with readers who approach studies of online environments from other perspectives.

Specifically, the focus here is on the phase in the development of the Internet often referred to as the «Web 2.0.» While there is not detailed agreement on what this supposed second stage of the World Wide Web entails, attempts towards a definition tend to revolve around ideas of increased user participation (e.g. O'Reilly, 2005). As suggested by Small, «Whereas Web 1.0 was 'read-only,' Web 2.0 is 'read/write,' allowing online users to contribute to the content rather than just being passive viewers» (Small, 2012: 91). Often discussed in conjunction with so-called social media services (such as Twitter or Facebook), services that are more or less dependent on such active user communities, the 2.0 variety of the Internet has received plenty of societal as well as scholarly interest – as well as its fair share of what must be labeled «hype.» The uses of such services, then, are often thought to yield «Big Data» – orderly traces of online activity of potential interest to researchers in multiple fields. While usage rates and modes of social media vary, these types of services are arguably here to stay – although we should not expect the services currently in fashion to remain so forever. What we can expect is for the data deluge created by these services to persist – and to grow in size.

While the term «Big Data» can be tagged onto a multitude of discussions regarding the increased possibilities of tracing, archiving, storing and analyzing online data, the specific appropriation of the term here deals with how masses of data are gathered from social media services like the ones discussed previously and subsequently analyzed for research purposes. In so doing, I would like to discuss two broad thematic groups of challenges that researchers often face when doing research on social media. The first group deals with

ethical issues, while the latter concerns more methodological possibilities and problems. Before delving into these issues, though, we need to look a bit closer at the term «Big Data» and its many connotations.

Big Data – size is everything?

As with the Web 2.0 concept, the term «Big Data» carries with it a number of differently ascribed meanings and ideas. As the name implies, definitions often involve discussions regarding the swelling size of the data sets that researchers as well as other professionals now have to deal with. Indeed, the growing use of social media combined with the increased sophistication of tools for «scraping» such online environments for data has provided «an ocean of data» (Lewis, Zamith, and Hermida, 2013: 35) that mirrors such new activities: Facebook updates, tweets, Instagram photos, etc. Such vast amounts of data can be collected and curated from a number of different services and with several purposes in mind – for scholarly efforts, this has led to claims like Chris Anderson's suggestion that Big Data could lead to «the end of theory» (Anderson, 2008). In essence, the quantities of data now readily available, supposedly at the click of a button, could render scholarly practices like employing theory and sampling rationales obsolete. While Anderson might be correct in that approaches to sampling and data collection more generally when it comes to research dealing with the online environment need to be revisited and reformulated in some instances, the argument is made here that no matter the vastness of the data, the need for some form of theoretical rationale in order to separate «noise from signal» (González-Bailón, 2013: 154) is evident. Indeed, searching for statistically significant correlations in large data sets could be considered an enlightening exercise in research methods, and might even lead to some initial observations

that could come in handy at a later stage in a given research project. But as with any collection of empirical data – big or small – one should also recognize the need for social theory to help provide context and guidance in order to separate meaningful relationships between variables from those that are unsubstantial (Silver, 2012).

It follows from this that while the scope of the data – the number of cases gathered and the number of variables employed – is of importance, size is perhaps not all that matters. As suggested by Margetts and Sutcliffe, «Big Data does not necessarily mean interesting data» (Margetts and Sutcliffe, 2013: 141), reminding us not to be blinded by size alone. As such, the quality of the data needs to be taken into account. Perhaps the ways in which data sets derived from social media activity allow for manipulation by the individual researcher should be the focal point. As these data tend to be structured in similar, coherent ways, and as our tools for analysis have grown in sophistication, size becomes an issue primarily with regards to sufficient or insufficient computing power. A large selection of empirical data is of course a good thing, and an absolute necessity in many research settings, but the quality of the data must be considered the first and foremost priority of the individual researcher.

Ethical considerations

Regarding ethical considerations pertaining to this type of research, I will raise three interrelated issues for discussion: (1) the «open» or «closed» nature of data, (2) communicating this type of research to ethics boards, and finally, (3) the need for respondent consent.

First, developments regarding computing power for collecting, storing and analyzing data are not showing signs of stopping or even plateauing. This implies that issues pertaining to the technical limits of the kind of operations that can be performed need to be

discussed in tandem with discussions of which types of activities should be performed We might label this a practical approach to research ethics.

As an example, we can point to some considerations that tend to arise when researching two of the currently most popular social media platforms, Twitter and Facebook. While the services differ in terms of modes of use, privacy settings and so on, we can distinguish between more «open» and more «closed» types of data from both platforms. For Twitter, users can add so-called hashtags – keywords formatted with a number sign (#) that signal a willingness on behalf of the user for their tagged tweet to be seen in a specific thematic context – that can assist researchers as well as other interested users in finding and selecting tweets of relevance. Such uses of hashtags are usually prevalent around the time of specific events, such as political elections, and have served as useful criteria for data collection in a series of studies (e.g. Bruns and Highfield, 2013; Larsson and Moe, 2012, 2013; Moe and Larsson, 2012b). However useful the hashtag criterion might be, there is a need to pose the question of what non-hashtagged content of relevance is available. We can readily assume that tweets that do not include these types of selectors may be of interest to researchers concerned with specific themes. While those types of messages could be gathered by using more open searches, we need to remember the aforementioned issue of the intent of the initial sender. The inclusion of hashtags can indeed be seen as a willingness on behalf of the sender to make the tweeted content publically available within a certain thematic context. While there are other, non-hashtag based modes of researching online political communication (e.g. Ausserhofer and Maireder, 2013), we need to take the open or closed nature of the data into account and shape our research approaches accordingly.

The same reasoning can (taking into account obvious differences regarding the specificities of the platform) be applied when dealing

with Facebook. Arguably a more locked-in service – a user essentially needs to have an account in order to gain access to most of the content – Facebook features Profiles, which is the type of Facebook presence most of us deal with in our everyday uses of the services. While Profiles are mostly associated with non-professional, personal Facebook use, professional employment has recently been taking place on so-called Pages. These Pages differ from Profiles in a number of ways – they are open to peruse by all, including by those who do not have a Facebook account, and they allow their respective owners (in this case, the political actors themselves) to extract more advanced metrics and information regarding usage rates than they would have been able to do if they had employed a personal Profile for professional matters. As with Twitter, we can differentiate between varying degrees of closed or open data here as well, where the operation of a Facebook Page at the hands of a political actor – be it individual parliamentarians, party leaders or even party accounts – could be considered a more open and public approach to the platform, thereby also making our job as researchers interested in the activities of politicians slightly less cumbersome. As general knowledge regarding privacy boundaries on Facebook are generally rather low (boyd and Hargittai, 2010), there might be issues regarding the degree to which activities of individual citizens interacting with politicians in these online spaces should be considered more or less public. The fact that many of the services available for Facebook data collection have built-in, non-revocable anonymizing features for users other than the Page owner should serve at least as a least temporary safeguard against privacy infringements when it comes to research on Facebook Pages. However, as these settings are very much in flux, researchers need to be aware of the specificities of the platforms they are interested in.

Second, the need for research ethics boards has been evident in basically all branches of scholarly activities in order to make sure

scholarly efforts meet the needs and standards set by society at large. While I have dealt with my own experiences regarding the relative difficulty of trying to communicate these issues to ethics boards in a separate, co-authored paper (Moe and Larsson, 2012a), some of these points need to be raised here as well. Essentially, two issues in particular could be raised when discussing ethics boards in combination with Big Data-type research. The first of these concern what could be labeled an «offline bias» in the many forms that need to be filled out when applying for these types of consultancies. As those forms have been constructed to reflect a research environment predominately geared towards research topics far from the specificities of online environments, researchers submitting their applications find themselves having to adapt their own descriptions to offline specifics in order to get the point of the research project across in a correct way. I am not necessarily suggesting that the forms should be extensively rewritten to fit issues pertaining to online research topics exclusively, but rather that those responsible for fashioning these channels for researcher input – be they printed or not – take some time to also adapt them for the many online themes that are currently on the rise within the social sciences and humanities. As such, perhaps these forms could become more specialized for specific types of research. The point here is not that research dealing with the online environment matters differs substantially from offline inquiries; rather, those differences that do exist need to be taken into account when dealing with research projects.

The second issue has to do with the varying degrees of feedback and transparency that characterize the decision-making process of ethics boards. While the information that needs to be submitted to these boards is often plentiful and requires significant amounts of legwork from the individual researcher, the degree to which the submitter gains insight into the reasoning of the ethics board, when they have reached their decision, is of a varying nature. While the

proverbial «burden of proof» should indeed lie on the researcher applying for ethical consultation, we also need to make sure that the feedback received – whatever the decision – is rich enough in detail so that the individual researcher can gain insight into the ways of reasoning applied. By securing at least some degree of transparency in these interactions, and by being more open in communicating these results to the academic community as well as to the general public, we will also be able to move towards precedents that will be very helpful for other, similarly interested researchers.

The third issue has to do with the necessity of obtaining consent when performing research on human subjects. While the practice of securing the willingness of those to be included in your study is more often than not a necessity, the practicalities of performing such operations must be raised for discussion when dealing with certain research projects. As an example, I would like to point to the work performed by myself and colleagues regarding political activity in conjunction with parliamentary elections in Sweden and Norway (Larsson and Moe, 2012, 2013; Moe and Larsson, 2012a, 2012b). While we did employ a hashtag-based mode of data collection, and while this fell in line with the stated regulations (Moe and Larsson, 2012a: 123), the Norwegian ethics board suggested that we attempt to obtain «non-active consent» from the Twitter users studied. We consulted our data sets and quickly realized that such an operation would involve contacting about 9000 Twitter users in order to receive their individual consent. After contacting the ethics board and explaining the situation, we were allowed to move on with our project without shouldering the massive workload of gaining such retroactive consent. Indeed, this signals a willingness on behalf of the entity to enter into dialogue with researchers, arguably a positive starting point. As the data collection was performed only with specifically hashtagged data in mind, this decision could be seen as relatively unproblematic – but we can be sure that there

are other situations – research regarding Internet use by minors, for example – where these issues are perhaps not as clear-cut.

Methodological considerations

As for challenges and questions pertaining to method when performing research on Big Data sets gathered from social media, I would like to raise four points in particular: the problem of «streetlight research,» the access to data, the stability of tools used, and finally, the competencies of researchers.

First, we can broadly conclude that among the many social media platforms available, Twitter and Facebook are (currently, at least) among the most popular, and as such, more interesting for researchers. As suggested by Lotan et al. (2011), the former of these services has indeed become quite popular among researchers – which more likely than not has to do with its accessibility in terms of how it allows for data from the service to be downloaded and archived. As such, the relative openness of the Twitter API (application programming interface) has led to a sizable number of studies dealing with this particular platform. While Twitter has put considerable restrictions regarding API access in place (e.g. Burgess and Bruns, 2012), it still must be considered more accessible than its arguably more popular competitor, Facebook. The relative ease of Twitter data collection, then, leads to what could be described as «streetlight research.» In essence, this is perhaps not a novel problem – we study what we can see, and try to make do with what is made available to us. But if the collective attention of researchers is largely directed at the second most popular service rather than at the one that boasts soaring usage rates by comparison, this could become a problem in the end. Ease of data access might be alluring, but the relative degree to which Facebook has been neglected in the same way creates a knowledge deficiency that does not serve the research community well.

Second, and related to the first point, is the problem of gaining access to data from a financial perspective. As both Twitter and Facebook have started to monetize access to certain parts of their respective APIs, partnering with third-party corporations to handle the day-to-day sales of data, it seems clear that finances will play an ever-increasing role in this type of research. For Twitter, this state of affairs can be illustrated by considering the different types of access allowed. While the so-called «firehose» API – including all the tweets sent through the service – is available, it carries with it a price tag that most academic institutions will not be able to pay. Instead, most researchers make do with what is labeled the «gardenhose» API – which provides a limited stream of tweets for free (e.g. Lewis, et al., 2013). The exact limitations of the latter API have been difficult to ascertain, but it has been suggested that the garden hose variety of access provides about one per cent of the total flow of tweets at any given time (e.g. Morstatter, Pfeffer, Liu, and Carley, 2013). As such, while we should not trust such «gardenhose» access to provide us with all data in a more general sense, more specified searches aimed at limited themes – such as the hashtag-based approaches discussed previously – should provide a fuller, more detailed data set. Of course, this is very much related to the expected scope of the hashtag examined. For Swedish or Norwegian contexts, where few citizens maintain an active Twitter account and fewer still take part in discussing political elections using the service, we can be sure to get a fuller picture than if we were to query the API for data on, say, a hashtag indicating tweets regarding a US presidential election. The key issue here is to be aware of the limitations that the tools employed for data collection carry with them and to shape one's studies accordingly. While a «garden hose» approach to data collection might be able to capture all tweets specified by a comparably limiting selection criterion, it will not be able to compete with the available commercial

services when it comes to the collection of tweets dealing with larger events – such as US presidential elections. Moreover, while such commercial services might be able to provide comprehensive sets of data even for more wide-reaching search queries, the ways in which such data are provided are often not conducive to further research efforts. While these data can provide useful initial insights, a researcher usually wants access to the raw data set. Commercially inclined customers might have these types of «ready-made» analyses as their primary goal, while this is often not the goal of the researcher. As such, even if researchers could afford to access firehose type data, the way they are presented is often not conducive to research purposes.

Third, the stability of the tools we use for data collection and analysis is of the utmost importance. While this is less of a problem for the latter of these activities, where open-source software such as Gawk (Bruns, 2011), Gephi (Bastian, Heymann, and Jacomy, 2009) or Netvizz (Rieder, 2013) sustain large user- and support communities, the former pursuit is arguably a bigger problem. In essence, as both Facebook and Twitter grow ever more popular, the way in which access to data through their respective APIs is granted is subject to more or less constant changes. Take Twitter as an example. As pointed out by Burgess and Bruns (2012), Twitter's changing business model has led to the collapse of a number of free services that were previously available to interested researcher. Facilities like 140kit and the web version of TwapperKeeper were essentially forced to remove certain functionalities from their services, effectively rendering them largely unsuitable for further use. While this problem has been partially solved by the launch of the user-hosted YourTwapperKeeper service (TwapperKeeper, 2010), stability still remains an issue as Twitter keeps changing their modus operandi on a more or less regular basis. If access to data remains unpredictable, this will continue to be a problem for researchers.

As a result of this lack of stability, a number of research teams have taken it upon themselves to build their own tools for data collection. While such tools are often impressive and attuned to the needs of the specific team, the uses of these types of «homebrew» software could lead to what is often referred to as a «silo problem» down the line. If each research team makes use of their own individually constructed data collection tools, ensuring comparability between research results could become a challenge. Although scholars have different needs with regard to the type of data they work with, there is a need for a point of comparison between teams. While total homogeneity is definitely not an ideal, a complete lack of comparative possibilities is definitely problematic.

Finally, the competencies of social scientists and humanities scholars for dealing with these sometimes novel issues of data collection and analysis need to be assessed. Indeed, the need for interdisciplinary efforts is perhaps more pressing than ever before (e.g. Lazer, et al., 2009). If we disregard the aforementioned suggested «end of theory,» the next step is perhaps to further realize what scholars working within the broader confounds of computer science can bring to the table. Theory is needed to pave the way, to find paths through vast quantities of data – but more technical skills are similarly needed to provide access to and manipulate the data in ways that make them receptive to the approaches of the social sciences and the humanities. Such cooperative efforts might not always be easy to carry out (e.g. Burgess and Bruns, 2012), but there is a clear need for them. Perhaps the suggestion by Margetts and Sutcliffe (2013) to provide a sort of «dating service» for different types of researchers could be one way to help bring about these sorely needed interdisciplinary activities. Such opportunities for researchers from different disciplines could be organized in conjunction with academic conferences or other similarly suitable meeting places.

In closing

The move to an online environment for social science and humanities research has indeed been fruitful for both branches. While the above considerations need to be taken into account when planning and executing a «Big Data» research project, they do not amount to a complete list. For example, the «siren-song of abundant data» (Karpf, 2012: 648) concerns the risk of the false impression of representativeness. While gauging Twitter streams and the like for the purposes of public sentiment analysis could prove an interesting methodological exercise (e.g. Groshek and Al-Rawi, 2013), researchers should be wary of making any brash conclusions concerning things to come based on social media data only. As the users and uses of social media in general, and Twitter in particular, tend to be characterized by varying sociodemographics (Hargittai and Litt, 2011; 2012), we must take such sources of bias – often geared towards societal elites – into account.

The issue of stability, mentioned above, is relevant to our understanding of the rather short history of social media platforms. Indeed, while Twitter and Facebook are currently among the more popular social media, this status is destined to come to an end when some novel service is launched and makes its claim for the online audience. With this in mind, researchers need to make sure that their instruments for inquiry – the way questions are posed or coding sheets are constructed – are «stress tested» and stable for future online platforms as well. This is almost certainly easier said than done. As rapid online developments take place, suitably aligned research instruments will enhance the quality not only of our present scholarly inquiries, but also of those to come in the future. Being prepared for these developments might help us in securing longitudinal insights regarding the uses of social media.

This chapter has outlined some of the considerations and challenges faced by researchers studying social media. While my specific starting point has been experience gained from my own

research into online political communication, it is my hope that the topics dealt with here also resonate with those interested in other areas. Finally, it must be mentioned that what has been presented here should not be considered an exhaustive list of issues to be dealt with – ideally, this piece will also serve as a conversation starter for moving on to those further issues.

References

Anderson, C. (2008, 23 June 2008). The End of Theory: The Data Deluge Makes the Scientific Method Obsolete. *Wired Magazine*, from http://www.wired.com/science/discoveries/magazine/16-07/pb_theory. Accessed 16 March, 2014.

Ausserhofer, J., & Maireder, A. (2013). National Politics on Twitter. *Information, Communication & Society, 16*(3), 291–314.

Bastian, M., Heymann, S., & Jacomy, M. (2009, May 17 – 20). *Gephi: An open source software for exploring and manipulating networks*. Paper presented at the Third International ICWSM Conference, San Jose, California.

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday; Volume 15, Number 8 – 2 August 2010*.

Bruns, A. (2011). How Long Is a Tweet? Mapping Dynamic Conversation Networks Ontwitterusing Gawk and Gephi. *Information, Communication & Society, 15*(9), 1323–1351.

Bruns, A., & Highfield, T. (2013). Political Networks Ontwitter. *Information, Communication & Society, 16*(5), 667–691.

Burgess, J., & Bruns, A. (2012). Twitter Archives and the Challenges of «Big Social Data» for Media and Communication Research. *M/C Journal, 15*(5).

González-Bailón, S. (2013). Social Science in the Era of Big Data. *Policy & Internet, 5*(2), 147–160.

Groshek, J., & Al-Rawi, A. (2013). Public Sentiment and Critical Framing in Social Media Content During the 2012 U.S. Presidential Campaign. *Social Science Computer Review, 31*(5), 563–576.

Hargittai, E., & Litt, E. (2011). The tweet smell of celebrity success: Explaining variation in Twitter adoption among a diverse group of young adults. *New Media & Society, 13*(5), 824–842.

Hargittai, E., & Litt, E. (2012). Becoming a Tweep. *Information, Communication & Society, 15*(5), 680–702.

Karpf, D. (2012). Social Science Research Methods in Internet Time. *Information, Communication & Society, 15*(5), 639–661.

Larsson, A.O., & Moe, H. (2012). Studying political microblogging: Twitter users in the 2010 Swedish election campaign. *New Media & Society, 14*(5), 729–747.

Larsson, A.O., & Moe, H. (2013). Twitter in Politics and Elections – Insights from Scandinavia. In A. Bruns, J. Burgess, K. Weller, C. Puschmann & M. Mahrt (Eds.), *Twitter and Society*. New York: Peter Lang.

Lazer, D., Pentland, A.S., Adamic, L., Aral, S., Barabasi, A.L., Brewer, D., et al. (2009). Life in the network: the coming age of computational social science. *Science, 323*(5915), 721–731

Lewis, S.C., Zamith, R., & Hermida, A. (2013). Content Analysis in an Era of Big Data: A Hybrid Approach to Computational and Manual Methods. *Journal of Broadcasting & Electronic Media, 57*(1), 34–52.

Lotan, G., Graeff, E., Ananny, M., Gaffney, D., Pearce, I., & boyd, d. (2011). The Revolutions were Tweeted: Information Flows during the 2011 Tunisian and Egyptian Revolutions. *International Journal of Communication, 5*, 1375–1405.

Margetts, H., & Sutcliffe, D. (2013). Addressing the Policy Challenges and Opportunities of «Big Data.» *Policy & Internet, 5*(2), 139–146.

Moe, H., & Larsson, A.O. (2012a). Methodological and Ethical Challenges Associated with Large-scale Analyses of Online Political Communication. *Nordicom Review, 33*(1), 117–124.

Moe, H., & Larsson, A.O. (2012b). Twitterbruk under valgkampen 2011. *Norsk Medietidsskrift, 19*(2), 151–162.

Morstatter, F., Pfeffer, J., Liu, H., & Carley, K.M. (2013, 2–4 June). *Is the Sample Good Enough? Comparing Data from Twitter's Streaming API with Twitter's Firehose*. Paper presented at the 8th International AAAI Conference on Weblogs and Social Media (ICWSM), Ann Arbor, MI, from http://arxiv.org/abs/1306.5204. Accessed 17 March, 2014.

O'Reilly, T. (2005). What is Web 2.0? Design Patterns and Business Models for the Next Generation of Software, from http://www.oreillynet.com/lpt/a/6228. Accessed 17 March, 2014.

Rieder, B. (2013, May 2–4). *Studying Facebook via Data Extraction: The Netvizz Application*. Paper presented at the WebSci'13 Conference, Paris, France, from http://rieder.polsys.net/files/rieder_websci.pdf. Accessed 17 March, 2014.

Silver, N. (2012). *The Signal and the Noise: Why So Many Predictions Fail–But Some Don't*. New York, NY: Penguin Press.

Small, T.A. (2012). e-Government in the Age of Social Media: An Analysis of the Canadian Government's Use of Twitter. *Policy & Internet, 4*(3–4), 91–111.

TwapperKeeper. (2010). Your TwapperKeeper – Archive your own Tweets, from http://your.twapperkeeper.com/. Accessed 17 March, 2014.

Big Data – big trouble?

Meanderings in an uncharted ethical landscape

Robindra Prabhu
Norwegian Board of Technology
robindra.prabhu@teknologiradet.no

Few concepts have made as many headlines in the past few years as the term «Big Data». From its nascent beginnings in technology circles, the term has rapidly catapulted into mainstream society. In recent years it has even become a household notion in the higher echelons of government: the Obama administration has launched its multi-million dollar «Big Data Initiative» (Office of Science and Technology Policy 2012), the United Nations has established a network of experimental labs exploring the possibility of leveraging Big Data for humanitarian purposes (United Nations Global Pulse), and recently the Australian government became one of the first in the world to launch a «Big Data Strategy» for its public service (Australian Government 2013).

With a promise to fundamentally «transform the way we live, work and think» through extensive «datafication» of all things human (Mayer-Shönberger, Cukier 2013: 73–97), Big Data vows to give us unprecedented insight into complicated problems and a powerful toolkit to better understand the world around us. With the

excessive hyperbole that is often associated with novel technology trends, one would be forgiven for mistaking the buzz for hype with little substance. And despite its ostensible potential, the significant amount of excitement it generates and the widespread agreement that Big Data will impact our society in crucial ways, there appears to be surprisingly little clarity concerning what Big Data actually is and what it entails for society at large.

So what is Big Data, anyway?

To be sure, there is no shortage of definitions. The «Big» alludes to unfathomable troves of digital data, in various shapes and forms, which we deliberately or passively generate in our daily interactions with technology. Then there is our enhanced ability to store, manage and extract insight from these data troves using powerful computing technology and the latest in advanced analytical techniques. But «Big Data» does not refer to a fixed quantitative threshold or clear-cut technological constraint. Indeed what is considered «big», «complex» and «advanced» varies widely. So much so that researchers have found it necessary to collate various definitions of the term «Big Data» and furnish the following meta-definition:

> Big Data is a term describing the storage and analysis of large and complex datasets using a series of techniques including, but not limited to: NoSQL, MapReduce and machine learning. (Ward, Barker 2013)

Perhaps it is only natural that early attempts to capture and define an allusive concept will come in many guises and possibly fall along a «moving technological axis». But while we struggle to pin down this new technology, it is important to recognise that Big Data's entry into the mainstream is equally about cultural changes in how we think about data, it's capture and analysis, and their rightful place in the fabric of society.

Whether hype or substance, and however most appropriately defined, the Big Data discourse is taking place against some profound (and I would argue exciting) changes in how we interact with our physical and social surroundings. These interactions invariably involve technologies and result in digital traces manifested in such various ways such as Internet clickstreams, location data from cell phones interacting with phone towers, data streams from credit card transactions, the logging of purchasing patterns in shops, the rich and multifaceted sensor data from an Airbus A380 in flight or vast detectors at research labs like CERN. Moreover, the emergent proliferation of low-cost sensors allows us to track and monitor objects and mechanisms in ways that were previously impossible. Farmers employ moisture sensors to monitor moisture levels in fields, shipments of fish and fruit are monitored for temperature and location in real-time as they are moved between continents, and people log personal health indicators using their smartphones.

Not only do we spend more time «online», but as we continue to add more «things» to the Internet, our lives become increasingly more entwined with the virtual world. And the digital traces we constantly leave behind in the virtual world now give us new handles on complex problems in the physical world.

The sceptic might demur that Big Data still has some way to go to deliver on its promise; targeted advertising and tailored movie recommendations may not appear to be the stuff of «revolutions». But fascinating applications are beginning to emerge: mobile phone data is being leveraged to map and track the spread of disease (Talbot 2013), law enforcement agencies are using predictive data-driven tools to determine the «where and when» of the next crime (The Economist 2013) and aggregate citizen sentiments are mined from large-scale social media feeds (Social Media and Post-2015) (Anderson 2008). In the future, more applications are likely to appear. And as we begin to deliberate on the wider ramifications of the rather nebulous

phenomenon of «Big Data», important clues for the ethical challenges ahead are likely to be found through close examination of the existing Big Data landscape. An appreciation of these challenges is not only of relevance to researchers who are dappling with new and vast troves of data, but also to private enterprises and governmental agencies looking to harness the power and potential of Big Data.

Treading ground between the enthusiasts and the sceptics

The nascent debate around Big Data may appear to be quite polarised. As Sandra González-Bailón remarks, the discussion on the proper governance and use of all these novel data sources has bifurcated public opinion into a two-pronged needle:

> … the sceptics, who question the legitimate use of that data on the basis of privacy and other ethical concerns; and the enthusiasts, who focus on the transformational impact of having more information than ever before. (González 2013: 147)

Both camps have extremists that will either dismiss the Big Data phenomenon as overhyped and underwhelming, or espouse the view that we are witnessing a new era in which the proliferation of data will render theory and interpretation superfluous (Anderson 2008) (Richards and King 2013).

While a healthy dose of both enthusiasm and scepticism is essential when dealing with new technologies, there are valuable lessons to be learned from the moderates on either side. Firstly, theory and interpretation are not likely to be discarded any time soon. Instead, their importance is reinforced as a sense-making tool in a growing sea of noisy data. Secondly, we would be wise to tread carefully, lest the critics are vindicated and we end up sleepwalking into a surveillance society.

As the debate and rhetoric advances and matures, it becomes important to capture the full range of nuanced challenges associated with the Big Data paradigm.

Moving beyond the hype: «Three paradoxes of Big Data»

An interesting turn in this direction is provided by Richards and King in their paper «Three Paradoxes of Big Data» (Richards and King 2013). While the authors do not deny the many benefits and the substantial potential inherent in Big Data, they advocate a more pragmatic discussion with due attention to the many faceted implications and inherent dangers of the Big Data paradigm by calling attention to three paradoxes in the current rhetoric:

1. *Transparency*: As sensors become ubiquitous and ever larger portions of our lives are mirrored onto a virtual world, enthusiastic proponents of Big Data argue that this pervasive data collection will serve to document the world as it is and make it more transparent.

   However, a fair portion of our personal data exhaust–small data inputs from sensors, cell phones, clickstreams and the like–are generally amassed into aggregated datasets «behind the scenes», largely without our knowledge. These datasets may in turn be saved in unknown and remote cloud services, where equally hidden algorithms mine the data for strategic insights. The paradox of this, they argue, is that if Big Data promises to make the world more transparent, then why is it that its «collection is invisible, and its tools and techniques are opaque, shrouded by layers of physical, legal, and technical privacy by design?» (Richards and King 2013: 42). Why, they argue, «is the Big Data revolution occurring mostly in secret?» (Richards and King 2013: 43).

While the authors acknowledge the need for trade secrets and the like, data collected from and used to make decisions about and on behalf of individuals merit the development of proper technical, commercial, ethical and legal safeguards. «We cannot have a system, or even the appearance of a system, where surveillance is secret, or where decisions are made about individuals by a Kafkaesque system of opaque and unreviewable decision-makers» (Richards and King 2013: 43).

2. *Identity*: Personalised services, exquisitely tailored to our individual tastes, needs and desires are a hallmark of the Big Data paradigm. Amazon leverages our browsing and purchasing history to group us with likeminded customers and provide us with customised shopping experiences. However, as these services gather information to identify «our true selves», there is a risk that the information is used to nudge us in a certain direction, different from where we would go if we were not under such influence. Google users, the authors argue, are «already influenced by big-data-fed feedback loops from Google's tailored search results, which risk producing individual and collective echo chambers of thought» (Richards and King 2013: 44). As Big Data actors leverage various data sources to identify «us», our right to define our own identity may be threatened. And without proper protections and safeguards against processes that minutely, incrementally and systematically undermine our intellectual choices, the authors argue «'you are' and 'you will like' risk becoming 'you cannot' and 'you will not'» (Richards and King 2013: 44).
3. *Power*: Enthusiasts often claim that Big Data will entail more transparency. Through the proper utilisation of new data streams, we are better placed than ever to shine a light on hidden processes and mechanisms – insight which in turn will allow us to generate an «X-ray» of the fabric of our society.

> However, as the authors point out, the tools and knowledge to wield these data streams, and to make inferences and decisions based on them, are currently in the hands of specialised intermediaries. They are not in the hands of the people who generate the data. Without a proper discourse around these challenges, the authors warn that this power asymmetry may result in «an uneasy, uncertain state of affairs that is not healthy for anyone and leaves individual rights eroded and our democracy diminished» (Richards and King 2013: 45).

The paradoxes framed around transparency, identity and power touch on more than one raw nerve in the current discourse on the ethical and societal implications of Big Data. A closer look at the various elements along the «Big Data chain» – namely data collection and storage, the application of analytical tools and finally action on the basis of insights mined–also reveals a host of potential shortcomings in current protective measures, as well as new challenges and problems.

Whose data is it anyway?

To date, most of the ethical concerns that have been raised relate to privacy challenges in the first link in the chain, namely that of the collection and storage of data. Many of these problems are not entirely new, but traditional mechanisms for ensuring privacy protection have come under increasing pressure with the advent of Big Data. Let us consider two cases:

1. The system of «notice and consent», whereby individuals are given the choice to opt out of sharing their personal data with third parties, has become a favoured mechanism of data protection. In practice, however, the online user is frequently met with lengthy privacy notices written in obscure legal language, where ultimately, she is presented with a binary choice to either accept

the complex set of terms or forsake the service in its entirety. The fatigue and apathy this generates is less than satisfying and it fails to bestow the individual with strong ownership over her data in any meaningful way. The problem is further exacerbated in the Big Data era because it places the onus of evaluating the consequences of data sharing on the individual generating the data. These evaluations can be both technical and complex, and individuals will necessarily be on unequal footing in terms of their ability to make informed choices. Therefore, researchers seeking to leverage e.g. social media data to study social systems cannot assume that they have tacit approval from users of these services – even if the consent agreement provides no legal impediments for such use. The key challenge lies in devising technical and regulatory frameworks that provide the user with tight and meaningful controls on personal data without compromising the practical utility of that same data.

Beyond the mere impracticability of the researcher having to actively seek consent from large swathes of people in all cases, some will argue that giving the data owner an absolute say in if and how her data is used runs the risk of interfering with the innovation potential of data use (Cate and Schönberger 2012; Narayana and Shmatikov 2006). All the possible use cases for a certain type of data (e.g. location data) are rarely apparent at the time of collection, which is when consent is typically sought. By tightly restricting the use of that data to certain predefined use cases, it is therefore likely that many useful applications we enjoy today, such as tracking tools that monitor traffic jams using cell phone movement, would never see the light of day (Sandberg 2012).

2. Another favoured privacy protecting measure is to anonymise datasets by stripping them of personally identifiable information before they are made available for analysis. While such

techniques might be privacy preserving when the dataset is treated in isolation, anonymised datasets have sometimes been shown to be easily de-anonymised when combined with other sources of information.

As part of a contest to improve its movie recommendation service, the online movie streaming service Netflix released an anonymised dataset containing the rental and rating history of almost half a million customers. By running the anonymised dataset against ratings on the online service «Internet Movie Database», researchers were not only able to identify individuals in Netflix's records, but also the political preferences of those people (Narayana and Shmatikov 2006).

There are similar examples of how an apparently anonymised dataset, when properly contextualised, is no longer truly anonymous. And the Big Data paradigm makes it increasingly more difficult to secure anonymity, because ever more data streams are generated, stored and made available for advanced data mining techniques (Navetta 2013). As the world becomes more data rich, researchers can no longer rest content with simplistic anonymisation to mitigate ethical risks.

Collect first, ask questions later …

The re-identification problem does not only highlight the shortcomings of established protective measures, but also shows that focusing exclusively on the proper governance of datasets and their attributes will often fall short of capturing the nuanced ethical challenges associated with data analysis. In order to grab the bull by the horns and provide the individual with meaningful control over personal information, it is necessary to govern *data usage* – that is, the actual operations performed on and with the datasets – rather than focusing solely on the collection and retention of such data. Doing so, however, is challenging, to say the least.

For while the current Big Data scene may appear to be dominated by a handful of major players, such as Google, Facebook and Amazon, its ecosystem is in fact highly distributed, with a host of third party actors operating behind the scenes which «often piggyback on the infrastructure built by the giants» (Sandberg 2012). Data collection, curation and analysis do not necessarily take place at a single point which can be subjected to robust regulatory measures.

Moreover, the technical opacity of algorithms underpinning Big Data analysis, as well as the real-time nature of such analyses, does not easily lend itself to meaningful scrutiny by way of traditional transparency and oversight mechanisms. In a world where

> … highly detailed research datasets are expected to be shared and re-used, linked and analysed, for knowledge that may or may not benefit the subjects, and all manner of information exploited for commercial gain, seemingly without limit. (Dwork 2014)

it can be hard to gauge *a priori* which operations are socially and ethically sound and which are not. Researchers may find that seemingly innocuous operations reveal themselves as privacy-intrusive or otherwise ethically «sticky» only after they have been performed. As computational techniques become increasingly more sophisticated and systems are able to extract personal information from datasets that appear harmless, relying on human intuition to define which operations are privacy-intrusive and which are not seems unsatisfying.

Can technology help to fix the problems it creates?

Technology is likely to be at least one part of the solution. Novel approaches such as «differential privacy» leverage mathematics to ensure both consistent and high standards for privacy protection in statistical operations on datasets involving sensitive data. Differentially

private algorithms satisfy mathematical conditions that allow the privacy risk involved in an operation on a dataset to be duly quantified. Once a threshold is passed the algorithm will intentionally blur the output so that individuals whose data are being analysed are ensured «plausible deniability». In other words, their presence or absence in the datasets in question has such a marginal impact on the aggregate result that there is no way of telling whether or not they were part of the dataset in the first place. Researchers can still draw value from the dataset because the «blurred» output differs only marginally from true output and the uncertainty, or «degree of blurring», is well known. Differentially private algorithms can also keep track of and appropriately quantify the cumulative privacy risk an individual sustains through repeated or multiple queries by iteratively adding more noise to mask any personal information residing in the data (Klarreich 2012).

Privacy and personal data protection are often touted as the central ethical challenges presented by Big Data. While technology may certainly help mitigate some of these risks, however, other challenges will require strong governance and legal protections. Furthermore, while we attend to the very pressing privacy concerns raised by Big Data, we should not lose sight of the many issues that fall outside the traditional privacy debate.

Looking beyond privacy

With recent technological advances, the cost of collecting, storing and analysing various kinds of data snippets has decreased quite dramatically. Novel methods also allow us to interlink and make sense of various kinds of data long after the data has been collected. As Alistair Croll remarks in an interesting blog-post: «In the old, data-is-scarce model, companies had to decide what to collect first, and then collect it. […] With the new, data-is-abundant model, we collect first and ask

questions later» (Croll 2012). This attitude was perhaps most amply illustrated by the mass surveillance activities of the NSA unravelled in the recent Snowden revelations, but it also holds true on a more general level. And this, Croll argues, is changing the way we use data.

Many remarkable successes of the Big Data paradigm, such as detecting disease outbreaks or predicting traffic jams, come from utilising data in ways that are very different from the original purpose of collection or the original context and meaning we bestowed on the data. However, Croll argues, this is a slippery slope fraught with ethical problems that go well beyond the regular privacy debate. Instead they deal with the inferences we are allowed to make and just how we act on or apply this insight. As the technical and financial barriers to what we can collect and do with data begin to crumble, the regulatory challenges to the proper use of data and analytics are likely to intensify (Soltani 2013).

As an example, Croll remarks on a study performed by the popular online dating service OkCupid, where the profile essays of some half a million users were mined for words that made each racial group in its member database statically distinguishable from other racial groups. According to the OkCupid blog post, «black people are 20 times more likely than everyone else to mention soul food, whereas no foods are distinct for white people» (Rudder 2010). The relatively simple study highlights just how easily information on race, sexual orientation, political standing or health can be inferred from innocuous information collected for very different purposes. Croll continues: «If I collect information on the music you listen to, you might assume I will use that data in order to suggest new songs, or share it with your friends. But instead I could use it to guess at your racial background. And then I could use that data to deny you a loan».

While such inferences may be partially construed as privacy issues–and legislative regulation can assist in preventing obvious transgressions–there are arguably deeper issues at play.

Inferences like the above are typically used to personalise and tailor adds, information, and online experiences to individuals. Such tailoring relies on classification–the algorithmic grouping of data points (people), and, as Dwork and Mulligan point out, such algorithms are a «messy mix of technical and human curating» and are «neither neutral nor objective», but always geared towards a specific purpose in a given context (Dwork and Mulligan 2013: 35). The objectionable or discriminatory outcome may not even be intentional or obvious to the providers of the service. As Sandberg remarks, a machine-learning algorithm trained on various data to determine the suitability of loan applicants, or even job applicants, may well «know» the race or political orientation of the applicant, even if it were not explicitly fed this information or programmed to use it. The information is baked into the data in non-obvious ways and ultimately «the algorithm will follow the data, not how we want to 'think'» (Sandberg 2012). Once differential treatment starts following certain social, political or religious patterns, the large scale effects on society can be profound. As Dwork and Mulligan argue, these issues have little to do with privacy and transparency, but are more about the «values embedded and reflected in classifications, and the roles they play in shaping public and private life» (Dwork and Mulligan 2013: 40).

Some cities across the U.S., notably Philadelphia, use statistical profiling techniques to determine the risk of criminal recidivism among parolees. The method relies on classification of offenders into groups for which certain statistical probabilities can be computed. While critics dismiss such methods as ethically questionable at best (should a cold calculus of past offences punish you for crimes you have not yet committed?), proponents argue that the method is not doing anything a parole board would not do, except with greater accuracy, with full absence of discriminatory urges and with more consistency and transparency.

The case highlights the challenging problems that we are likely to face as Big Data moves out of its nascent stage of tailored ads to affect a wider range of human activity. It also shows how easy it is to fall prey to the temptation of framing the problem as one of man versus machine. Such an approach is likely to be counter-productive. The challenge of managing «ethical risk» in a Big Data world is one that is jointly technological and sociological, and as Dwork and Mulligan succinctly put it: «[…] Big Data debates are ultimately about values first, and about math and machines only second» (Dwork and Mulligan 2013: 38).

Moving forward

Like other technologies in the past, as Big Data unfolds and is absorbed into society we are likely to see adjustments and changes in our current notions of privacy, civil liberties and moral guidelines. And as the hype eventually wears off and a proper equilibrium between the role of human intuition and data-driven insight is established, we will need to develop tools, guidelines and legislation to govern this new world of data and data analysis. This process will require a wide perspective, coupled with constant and close scrutiny of all links along the Big Data chain. It is an arduous task, but also one that should be exciting for all involved. Future societies might be shaped by technological advances, but technology itself is moulded by human choices. And these choices are available for us to make now.

References

Anderson, C. 2008. «The End of Theory: The Data Deluge Makes the Scientific Method Obsolete». Available from http://www.wired.com/science/discoveries/magazine/16-07/pb_theory (accessed February 24, 2014).

Australian Government. «The Austrialian Public Service Big Data Strategy». Department of Finance and Deregulation, 2013.

Cate, F.H. and Mayer-Schönberger, V. 2013. Notice and Consent in a World of Big Data. International Data Privacy Law, 3 (2): 67–73.

Croll, A. «Big data is our generation's civil rights issue, and we don't know it.» *radar.oreilly.com*. August 2, 2012. http://radar.oreilly.com/2012/08/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it.html (accessed February 24, 2014).

Dwork, C. 2014 Differential Privacy: A Cryptographic Approach to Private Data Analysis (private communication).

Dwork, C. and Mulligan, D.K. 2013. It's Not Privacy, and It's Not Fair. *Stanford Law Review Online* 66, no. 35: 35–40.

González-Bailón, S. 2013. Social science in the era of big data. *Policy & Internet* 5: 147–160.

Klarreich, E. 2013. Privacy by the Numbers: A New Approach to Safeguarding Data. http://www.scientificamerican.com/article/privacy-by-the-numbers-a-new-approach-to-safeguarding-data/ (accessed February 24, 2014).

Mayer-Schönberger V. and Cuckier, K. 2013. Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt.

Narayana, A. and Shmatikov, V. «How To Break Anonymity of the Netflix Prize Dataset.» *CoRR*, 2006. http://arxiv.org/pdf/cs/0610105.pdf (accessed February 24, 2014).

Navetta, D. 2013. The Privacy Legal Implications of Big Data: A Primer. http://www.infolawgroup.com/2013/02/articles/big-data/the-privacy-legal-implications-of-big-data-a-primer/ (accessed February 24, 2014).

Office of Science and Technology Policy, Executive Office of the President. 2012. «www.whitehouse.gov.» http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release.pdf (accessed February 24, 2014).

Richards, N.M. and Jonathan H.K. 2013. Three Paradoxes of Big Data. *Stanford Law Review Online* 66, no. 41: 41–46.

Rudder, C. 2010. The REAL «Stuff White People Like». http://blog.okcupid.com/index.php/the-real-stuff-white-people-like/ (accessed February 24, 2014).

Sandberg, A. 2012. Asking the right questions: big data and civil rights. August 6, 2012. http://blog.practicalethics.ox.ac.uk/2012/08/asking-the-right-questions-big-data-and-civil-rights/ (accessed February 24, 2014).

Social Media and Post-2015. 2013. post2015.unglobalpulse.net.

Soltani, A. 2013. Soaring Surveillance. http://www.technologyreview.com/view/516691/soaring-surveillance/ (accessed February 24, 2014).

Talbot, D. 2013. *Big Data from Cheap Phones*. http://www.technologyreview.com/featuredstory/513721/big-data-from-cheap-phones/ (accessed February 24, 2014).

The Economist. 2013. Predictive Policing: Don't even think about it. http://www.economist.com/news/briefing/21582042-it-getting-easier-foresee-wrongdoing-and-spot-likely-wrongdoers-dont-even-think-about-it (accessed February 24, 2014).

United Nations Global Pulse. www.unglobalpulse.org.

Ward, J.S. and Barker, A. 2013. Undefined By Data: A Survey of Big Data Definitions. http://arxiv.org/abs/1309.5821, (accessed February 24, 2014).

About the authors

Dag Elgesem, Professor of ICT and Society at the Department of Information Science and Media Studies, University of Bergen. He has been working on normative issues related to ICT, including Internet research ethics, for a number of years. His current research focuses on methods for the analysis of discourses in social media, in particular blogs, and he leads the project Networks of Texts and People (ntap.no). From 1995 to 2000 he was the director of NESH.

Bernard Enjolras is head of research at the Institute for Social Research in Oslo and research director at the Centre for Research on Civil Society and Voluntary Sector. He has a PhD in sociology from the Université du Québec à Montréal (Canada), and a PhD in socioeconomics from Paris-Sorbonne University (France). His fields of research are civil society, non-governmental organizations, public policy, public governance, social media and the public sphere.

Charles Ess, (PhD, Pennsylvania State University, USA) is Professor in Media Studies, Department of Media and Communication, University of Oslo, and Emeritus Professor of Philosophy and Religion, Drury University (Springfield, Missouri), USA. Emphasizing cross-cultural perspectives, Dr. Ess has published extensively in the field of information and computing ethics and Internet studies.

Anders Olof Larsson is currently a postdoctoral fellow at the Department of Media and Communication, University of Oslo.

Larsson's research interests include the use of the Internet by societal institutions and their audiences, online political communication and quantitative methods. For more information, see www.andersoloflarsson.se

Marika Lüders, (PhD, UiO) is a senior research scientist at SINTEF, Oslo. Her research concerns the consequences of the networked society, addressing e.g. social network sites, knowledge-sharing, democratic participation and privacy. Her work has been published in journals such as New Media & Society and Journal of Computer-Mediated Communication.

Robindra Prabhu is a project manager with the Norwegian Board of Technology. His work centres on policy opportunities and challenges related to Big Data, machine learning, algorithmic predictions and decision-making, and their wider implications for society. He was previously a Research Associate at University College London, working on data analysis and the development of algorithmic tools for the Large Hadron Collider project at CERN, and holds a PhD in high energy physics.

Katrine Utaaker Segadal is a social scientist and the Head of Section for the Data Protection Official for Research at the Norwegian Social Science Data Services (NSD). She works with ethical and legal issues regarding privacy protection, with a focus on sustaining needs of research within the regulatory framework.

Elisabeth Staksrud, PhD, is Associate Professor and Head of Studies at the Department of Media and Communication, University of Oslo, researching censorship, media regulation, children and online risk. She is also deputy chair of NESH. Her most recent publication includes "Children in the Online world: Risk, Regulation, Rights" (Ashgate, 2013), "Towards a better Internet for children?" (O'Neill, B., Staksrud, E., & McLaughlin, S. (Eds.), 2013, Nordicom), and a book on online bullying ("Digital Mobbing", Kommuneforlaget, 2013).

Kari Steen-Johnsen, Ph.D, is Research Professor at the Institute for Social Research, Oslo. She is a sociologist with a particular interest in changes within civil society. In her recent research she explores the impact of digitalization on political participation, democracy and the public sphere.