Handbook Ethics

20 June 2016
version 1.2

UNIVERSITEIT VAN AMSTERDAM

Introduction

Until very recently, ethical discussions were only relevant to fields of research in which research is conducted directly on humans, such as medicine and some social sciences. However, due to the increased involvement of humans as (in)direct research objects in the Information Sciences (IS), these ethical discussions are also becoming important in this field.

For instance, socials scientists might use online social media as tools for their research. This often leads to discussions about the privacy of data. This new type of research thus creates dozens of new questions, such as…

1) How is the autonomy of all participants guaranteed?
2) How do we know if a participant has understood the objectives of the project?
3) Do the participant and the researcher have the same ideas about private versus public? (especially relevant where social media is conducted)
4) How are research data protected?
5) By whom and how can data be found and read?

On the other hand, information scientists sometimes conduct research into the access to and security of networks and are thus likely to find vulnerabilities in information systems. This also creates a lot of questions, such as…

1) Should the owner of the investigated Information System be aware of this investigation?
2) Which methods (ethical or not) are being used to access the system?
3) How should the discovery of a vulnerability be treated?
4) How should information be disclosed?

Despite the fact that these two examples have not been chosen arbitrarily, the problem is very clear.

The integrity of the researchers and this research can thus only be guaranteed if these aspects are looked at more closely. They need a framework within which to work and if research is indeed conducted within this framework, the Informatics Institute will then be able to be supportive of and take responsibility for the research.

In other words, to guarantee the quality and social relevance of research conducted under the umbrella of the Informatics Institute, the legal and ethical aspects of research need to be examined before, during and after the project. This will be done by the Ethical Committee for Information Sciences (ECIS), which is part of the Institute for Information Sciences of the University of Amsterdam. Research will, for these purposes, be divided into standard and non-standard research based on the nature of the research.

Part I

Definitions

Standard research within the Informatics Institute

A new research project may only be classified as standard research within the Informatics Institute if it satisfies all of the conditions of the applicable field as set out in Appendix I (?). In the case of standard research, submission of the research proposal to the secretary of the ECIS will be adequate.

Non-standard research within the Informatics Institute

All research that fails to satisfy one or more of the conditions of standard research.

Theoretical research within the Informatics Institute

Research that does not require interaction with external groups.

Controversial aspects

All aspects that have been or are likely to be prone to ethical and/or legal problems.

Statute

1. If a research project is to be conducted under the authority of the Informatics Institute and is either non-standard or includes controversial aspects (see appendix I), it is required to be presented to the Ethical Committee Information Sciences (ECIS) prior to the commencement of the study. This applies to members of staff, as well as to postdocs and students. At all times a project needs to be approved by the ECIS in order for the Informatics Institute to be able to take (partial) responsibility for the undertaking. The main person in charge of the project will always be a researcher who works for or has been admitted to the Informatics Institute. In the case of students, interns or external employees conducting research, somebody belonging to the Informatics Institute should take responsibility for the project. Additionally, research conducted elsewhere by an Informatics Institute member (and thus on behalf of the Informatics Institute) requires approval.
2. The ECIS has set up rules for the process of conducting research. These can be found on ecis.ivi.uva.nl. The decision whether to grant approval to a project is made based on these rules. The Informatics Institute does not take responsibility for projects that have not been presented to the Informatics Institute, which means that the researcher will be directly responsible for the project. The rules may change over time due to new experiences within and beyond a particular field of research, which means that a project may require reassessment at any given time. The ECIS always has the final say on the approval or rejection of a research proposal and reserves the right to (in highly exceptional cases) cut off research that has been approved in the past.
3. The ECIS strives to make the application process as straightforward as possible in order to minimise the delay of research progress. Additional administrative work for the researcher will also be avoided as much as possible. If a new research proposal

satisfies all the guidelines of standard research, going through the accelerated application process will be sufficient. In that case, the director of the ECIS is authorised to give provisional approval, whereas the normal procedure requires the permission of the whole ECIS before a definite go-ahead can be given.

4. The ECIS is comprised of four reputable members of staff who are appointed for a one- year term. They are responsible for at least one branch of the institute, although never the one they themselves are affiliated to. The director of the Informatics Institute is the chair of the ECIS and is assisted by a secretary and lawyers. The ECIS meets six times a year, or if necessary for the advance of a project more often, to discuss research proposals and possible policy changes.
5. Proposals that require the attention of the full committee (and thus cannot go through the accelerated procedure) will be discussed at the first upcoming meeting unless there are pressing arguments for prompt consideration. Thus, approvals will always be granted or denied within two months, unless further information about the project is has been asked for and hasn't been submitted within the required timeframe.
6. Formally the research policy has been mandated to the director of the Informatics Institute. He is responsible for the quality as well as the scientific orientation of the institute and thus affirms the ECIS. This policy fall under administrative law and is thus also subject to those appeal procedures.

How to submit a research proposal to the ECIS

1. To ensure a smooth assessment process, the researcher should have an idea as to which sub-department his or her research might belong to. However, the final decision on this will be made by the relevant ECIS member. Usually researchers in a certain department will have experience in a particular research area, so if they are not familiar with the type of research that has been proposed, it is more likely that the ECIS will need to consider the case more closely.

   The different sub-departments and associated types of standard research can be found in Appendix I.

2. Complete the checklist (Appendix II). The general section should be completed first, followed by the section of the sub-department which the project will (most likely) be part of.
   The questions ought to be answered honestly. In addition to that, the questions are not meant to be taken literally, i.e. formulations should not be interpreted in implausible ways in order to gain personal advantage. Moreover, in the case of even the slightest bit of doubt this should be mentioned in the answer. This is especially important for questions related to whether the project can or cannot be classified as standard research. Due to the nature of research, it is obviously impossible to provide a description of every single type of research. Nonetheless, do not classify your research as standard research unless it matches <u>all</u> the given criteria.

   The results of the checklist will determine whether the proposal is eligible for the accelerated procedure (3a) or not (3b).

3.
   a. The accelerated procedure only requires the researcher to submit the questionnaire and required information to the secretary of the ECIS. The secretary will send a confirmation upon receiving and delegate the proposal to the relevant ECIS member. This member will announce the outcome to the researcher via email and also send a copy of the outcome to the secretary.
   b. The full procedure requires the researcher to send a summary of the project to the secretary of the ECIS. At the very least, this summary should clearly show the ways in which this research is not ‘standard research’. If the project would be classified as standard if it were to be conducted under another branch, this should be mentioned.

      In all cases, the ECIS member of the relevant department will present the proposal to the full committee. The ECIS may decide to organize an immediate meeting, or otherwise to wait until the next scheduled meeting. In the meantime, the relevant ECIS member is entitled to give provisional permission for the researcher to start the project. However, final* permission can only be given after the whole committee has been consulted. In the unfortunate case of rejection, the reasoning behind this will be disclosed and suggestions for improvement may be given.

      *Ongoing research may turn out to have new and/or unexpected aspects that require more consideration by the ECIS. In this case, the secretary of the ECIS should be informed promptly. He will then decide whether the case requires immediate action.

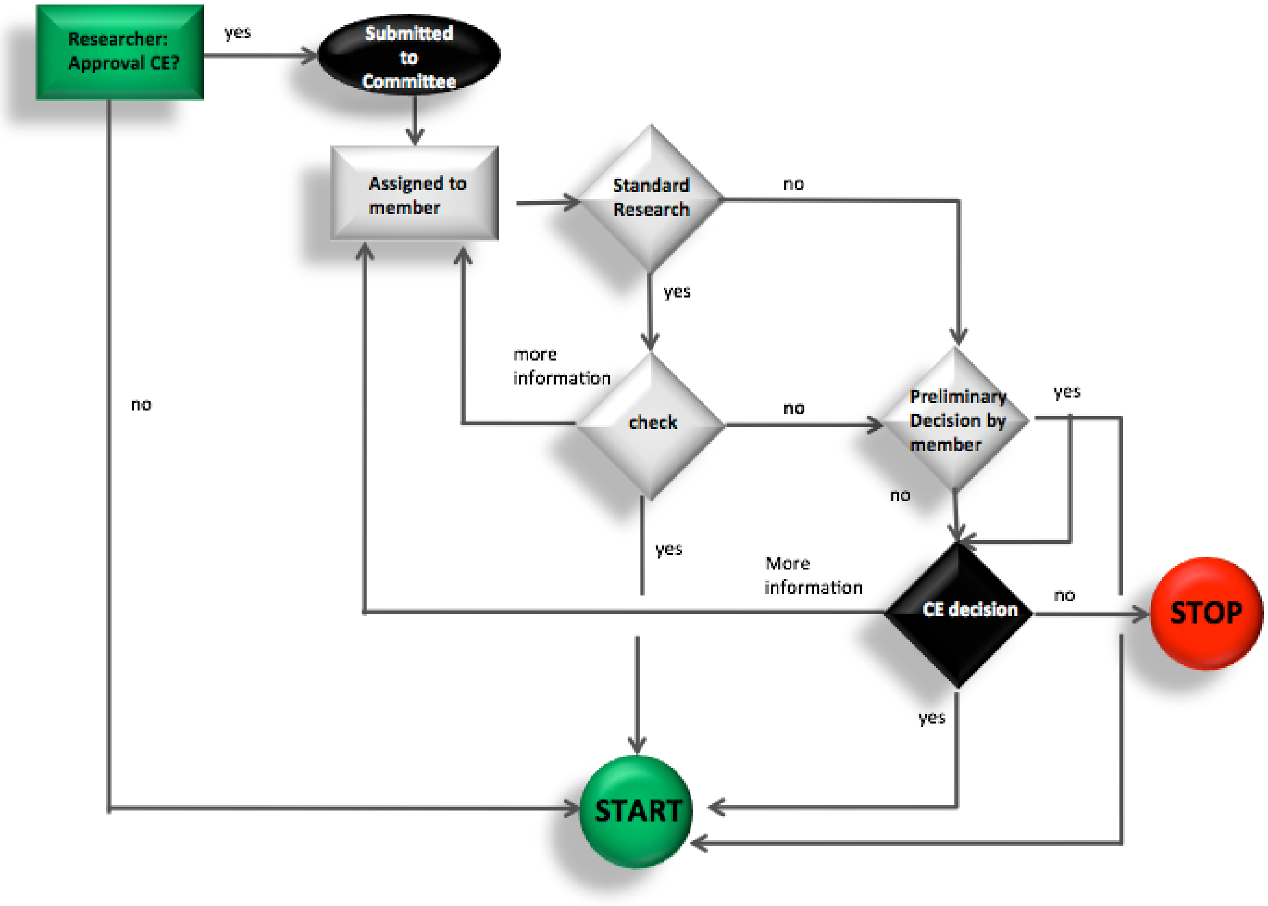

figure 1. Flowchart

Legal aspects

Researchers who find a vulnerability in a system, are responsible for their own actions and thus for the methods that were used to find this vulnerability. If the discovery of the vulnerability involved the commitment of crime(s), reporting this discovery will reduce but not fully eliminate the chances of prosecution.

The chances of prosecution can be limited even more if the finder doesn't commit a crime in the process. This can be prevented by following these guidelines:

- Don't utilize social engineering to get access to a system. This is a technique based on finding and attacking the weakest link in the system, which is always a human. The goal of the attack is to gain access to confidential or secret information that can then be used to gain access to the computer system.
- Don't construct a backdoor in a system just for the sake of finding a vulnerability in the system. This may cause further damage and often leads to additional security risks.
- Don't use a vulnerability for any other purpose than to demonstrate the its presence.
- Don't copy, change or delete any data in the system. If need be, a directory list can be made instead.
- Don't make any changes to the system
- Don't try to repeatedly gain access to the system and don't share this access with others.
- Don't brute force access to systems. This technique just entails continually trying different passwords and is thus unnecessary and inappropriate for discovering vulnerabilities.

Publication

Responsible disclosure

The communication with the owner of a system containing a vulnerability is a delicate process. This is due to the large mutual interests, such as potential damage to the system, reputation damage and the potential for publication by students. Thus, good guidance and support of researchers (or those representing them) in this process is important.

Typically, the *responsible disclosure* method is utilized to communicate with the relevant organisation. This entails *full disclosure*, but provides the disadvantaged body with time to solve the problem before the information is published. The amount of time and level of disclosure depend on the potential impact of the vulnerability.

The process of finding and communicating a vulnerability is comprised of three different phases:

Research phase

This is the phase in which the vulnerability is found. If the applied methods may cause legal or ethical problems, the gravity of these problems needs to be determined. In the case of research by students, a teacher will be responsible for this process. If there are any difficulties, juridical advice should be sought. In the meantime, complete secrecy is required.

Communication phase

Prior to the publication of the discovery, the company needs to be fully informed about the problem and associated risks. The finder (see example) is fully responsible for this. If need be, a third party may get involved. In order to avoid leakage of information this communication must be entirely confidential.

The next step is to determine the amount of time to be given to the company to fix the problem. Usually they are given about 30 days, but this is negotiable. In addition to that, the extent to which the information should remain confidential needs to be determined. During this phase, communication should be fully transparent and all information required to reproduce the vulnerability needs to be made available.

Every phase of the communication process needs to be recorded.

End phase

When both parties have confirmed that the problem has been solved, the information may be published.

Appendix II contains an detailed example of a procedure(?).

Publication

Responsible disclosure

The communication with the owner of a system containing a vulnerability is a delicate process. This is due to the large mutual interests, such as potential damage to the system, reputation damage and the potential for publication by students. Thus, good guidance and support of researchers (or those representing them) in this process is important.

Typically, the *responsible disclosure* method is utilized to communicate with the relevant organisation. This entails *full disclosure*, but provides the disadvantaged body with time to solve the problem before the information is published. The amount of time and level of disclosure depend on the potential impact of the vulnerability.

The process of finding and communicating a vulnerability is comprised of three different phases:

Research phase

This is the phase in which the vulnerability is found. If the applied methods may cause legal or ethical problems, the gravity of these problems needs to be determined. In the case of research by students, a teacher will be responsible for this process. If there are any difficulties, juridical advice should be sought. In the meantime, complete secrecy is required.

Communication phase

Prior to the publication of the discovery, the company needs to be fully informed about the problem and associated risks. The finder (see example) is fully responsible for this. If need be, a third party may get involved. In order to avoid leakage of information this communication must be entirely confidential.

The next step is to determine the amount of time to be given to the company to fix the problem. Usually they are given about 30 days, but this is negotiable. In addition to that, the extent to which the information should remain confidential needs to be determined. During this phase, communication should be fully transparent and all information required to reproduce the vulnerability needs to be made available.

Every phase of the communication process needs to be recorded.

End phase

When both parties have confirmed that the problem has been solved, the information may be published.

Appendix II contains an detailed example of a procedure(?).

Publication

Responsible disclosure

The communication with the owner of a system containing a vulnerability is a delicate process. This is due to the large mutual interests, such as potential damage to the system, reputation damage and the potential for publication by students. Thus, good guidance and support of researchers (or those representing them) in this process is important.

Typically, the *responsible disclosure* method is utilized to communicate with the relevant organisation. This entails *full disclosure*, but provides the disadvantaged body with time to solve the problem before the information is published. The amount of time and level of disclosure depend on the potential impact of the vulnerability.

The process of finding and communicating a vulnerability is comprised of three different phases:

Research phase

This is the phase in which the vulnerability is found. If the applied methods may cause legal or ethical problems, the gravity of these problems needs to be determined. In the case of research by students, a teacher will be responsible for this process. If there are any difficulties, juridical advice should be sought. In the meantime, complete secrecy is required.

Communication phase

Prior to the publication of the discovery, the company needs to be fully informed about the problem and associated risks. The finder (see example) is fully responsible for this. If need be, a third party may get involved. In order to avoid leakage of information this communication must be entirely confidential.

The next step is to determine the amount of time to be given to the company to fix the problem. Usually they are given about 30 days, but this is negotiable. In addition to that, the extent to which the information should remain confidential needs to be determined. During this phase, communication should be fully transparent and all information required to reproduce the vulnerability needs to be made available.

Every phase of the communication process needs to be recorded.

End phase

When both parties have confirmed that the problem has been solved, the information may be published.

I. Appendix II contains an detailed example of a procedure(?).

Appendix I

Appendix II

Generic questions

Basic information

1. Title of the project
2. Person in charge (incl. professor in the case of PhD's)
3. Conducting researchers
4. Sub-department
5. Location of project execution
6. Short description of the project
7. Names of organisations involved
8. ECIS member of the relevant sub-department

Questions

9. Have you proposed this or a similar project to the ECIS in the past
    - o Yes
    - o No
10. Will external objects be involved in the project?
    - o Yes
    - o No

    If so, are the objects owned by research partners?

11. Is the owner of the object aware of this project?
    - o Yes
    - o No

    If not, why not?
12. Has juridical advice been provided?
    - o Yes
    - o No

    If yes, please attach the advice
13. If the information has been disclosed, has an agreement for future steps been reached?
    - o Yes
    - o No

    If yes, with whom and what?
14. Is the project likely to attract attention from the media?
    - o Yes
    - o No

    If so, please describe the nature of this sensitivity.

Specifieke vragen

Commercial web services (data storage))

1. What are the participant/author's expectations of privacy?

2. Is the data easily searchable and retrievable? Is the data subject to open data laws or regulations?

3. Does the service’s privacy policy contradict ethical principles?

4. What measures safeguard data at the site of data collection?

5. How long will the data be stored on the servers?

6. Does this contradict the time frame indicated by the researcher or institutional policies?

7. What happens to the data after the researcher completes work on the service?

8. How are the data destroyed?

9. How will cross---border data be handled if IP addresses are considered by one country to fall under privacy regulations?

Databanks

10. Where is the data stored?

11. How long will the data exist in the repository?

12. What consent is needed for subsequent data use?

13. Does the remixing/mashing of data enable identification of individual or group identities or enable any additional risks to participants?

14. In the case of shared data, what conditions were placed on data use by the original researcher, if any?

15. Regardless of conditions, what ethical responsibilities may require consideration by later users?

16. What mechanisms are in place to ensure appropriate data provenance and ownership?

17. How will images/audio be effectively anonymized?

Security

18. Are you searching for a vulnerability in a network or application?

19. Does the owner of the information system knows you are searching for vulnerability?

20. Are the activities in conflicts with regulations?

21. Which law applies? Dutch, American………?

22. What is the impact of the vulnerability?

23. Does the vulnerability affects anyone privacy ?

24. How do you communicate with the owner of the vulnerability?

25. How can researcher ensure that author/participant understands and agrees that content or interaction may be used for research purposes?

26. Is the communication archived or easily searchable and retrievable?

27. Is the data subject to open data laws or regulations?

28. How long does the third party provider or ISP preserve the data and where?

29. Could privacy be achieved through anonymization of email content and/or header information?

Special interest forums

30. How do terms of service (TOS) articulate privacy of content and/or how it is shared with 3rd parties?

31. Regardless of TOS, what are community or individual norms and/or expectations for privacy?

32. Does the author/subject consider personal network of connections sensitive information?

33. Is the data easily searchable and retrievable?

34. If the content of a subject's communication were to become known beyond the confines of the venue being studied – would harm likely result?

35. Is the conversation thread or forum perceived as public or private by the author(s)/subject(s)?

36. How is profile, location, or other personally identifying information used or stored by researcher?

37. Is the data easily searchable and retrievable?

38. How is informed consent or protection of privacy achieved?

39. How are vulnerable persons identified and protected?

40. If non---active archives are used, how is vulnerability or harm defined and how are potential or actual subjects protected?

Social networking

41. How do the terms of service articulate privacy of content and/or how it is shared with 3rd parties?

42. Does the author/participant consider personal network of connections sensitive information?

43. How is profile or location information used or stored by researcher?
    Does author/participant understand and agree to interaction that may be used for research purposes?

44. Does research purpose and design balance possible conflicts between participant and researcher

perceptions of public/private and sensitive/non sensitive?

45. Does the dissemination of findings protect confidentiality?
46. Is the data easily searchable and retrievable?
47. If the content of a subject's communication was ever linked to the person, would harm likely result?

Personal spaces

48. Could analysis, publication, redistribution, or dissemination of content harm the subject in any way?
49. If the content of a subject's communication were to become known beyond the confines of the venue being studied would harm likely result?
50. Does the author/participant consider personal network of connections sensitive information?
51. Does author/participant consider the presentation of information or venue to be private or public?
52. Do the terms of service conflict with ethical principles?
53. Is the author/subject a minor?

Virtual worlds

54. Should these virtual worlds be considered "public"?
55. What constitutes "privacy" in such places?
56. Should avatars be considered as persons and afforded the same protections as human subjects?
57. .Will the process of requesting consent itself cause harm?
58. How and when should consent be sought?
59. What requires consent?
60. To what extent do users perceive their interactions and communication to be private in these spaces?
61. How do Terms of Service specify researcher presence, anonymity of users, and privacy/ confidentiality?
62. To what extent and in what ways could research activities interfere with or compromise a user's play or outcomes in the game?

63. How should researchers juggle their own multiple roles?

64. Could data be used to identify a user’s physical location and other sensitive demographic information?

Appendix III

Initial communication example

Dear Sir/Madam,

As part of a project counting towards a master's degree in System and Network Engineering from the University of Amsterdam, students have been conducting research into the security of different mobile applications, such as X.

The study has revealed a couple of security issues which require your immediate attention. We think we have found a vulnerability in your application for Androids which may enable personal information…blablabla…. These findings have been kept confidential and all the rules stated by the National Cyber Security Center (NCSC) were adhered to during this research.

We would like to show these outcomes to you and give you the chance to fix these problems, before we publish this information. During our communication process, we aim to act according to the 'Guidelines to setting up Responsible Disclosure'.

Thus we invite you to get in touch with us promptly by responding to this email. Best wishes,

Procedure after discovering a vulnerability

1. The chair of the Informatics Institute will appoint a process coordinator (PC). Given the required subject-specific knowledge, leadership skills and diplomacy, this will likely be a senior member of staff. He or she will be required to oversee and encourage the process, in addition to keeping the executives(?) of the institution informed. All further actions (including publication) need to be approved by the PC.

2. It needs to reported whether the research was conducted in an legal and ethically responsible manner (action PC and potential lawyer)

3. A letter needs to be written containing the findings as well as a proposal for responsible disclosure. This can take place in a hierarchical (?) manner:
    a. Operational Level (action supervisor)
    b. Strategic level (action course director)

    They may be supported by a lawyer and if needed a communication advisor. The latter may ensure that the letter is written correctly.

4. The letter should be shown to the dean of the FNWI if the PC has demanded this.

5. At the end of the process, the results may be published. A popular (i.e. understandable for non-computer scientists) version of the paper is required for internal objectives.