The USENIX Journal of Education in System Administration
Volume 1, Number 1 • September 2015
www.usenix.org/jesa/0101

Embedding Ethics in System Administration Education

Jeroen van der Ham, National Cyber Security Centre-NL, University of Amsterdam

Ethics is an important part of education in system administration. It is a hard subject to teach to science students, yet it is a pervasive issue in system administration and especially security research. Many student research project will touch on the security of users, their private data, or can even have implications for physical security.

In this article we demonstrate our approach for teaching and evaluating ethics. We start with regular lectures in ethics, but follow up with practical training by forcing the students to write ethical consideration paragraph in all of their project proposals. These proposals are then evaluated by an ethics committee for this educational programme. The ethics advisor is involved in supervising the project depending on the outcome of the ethical evaluation.

In this paper we also discuss several proposals that were submitted to the ethics committee. We discuss the deliberations, the eventual categorisation of the project, but also the outcomes of the projects. With these case descriptions we would like to improve the discussion on ethical aspects of system administration and security research.

1. INTRODUCTION

Computer scientists and engineers have long felt that ethics is an important part of their job: communities such as USENIX [Committee 2003], and the ACM [council 1992] have published codes of ethics. With the increasing popularity and dependency on the Internet, so too did interest in ethics in security research increase [Bailey and Kenneally 2014b][Bailey and Kenneally 2014a].

The System and Network Engineering Master education at the University of Amsterdam is a one year programme. In this limited time, students learn the theoretical underpinnings of networking, security, forensics and other related topics. The programme is designed so that students receive classical lectures in the morning. The rest of the day also consists of lab exercises: students must run their own servers, and do exercises. Most of the 12 courses contain a small project that the students do in teams or alone. Many of these projects are related to security or possibly sensitive data.

The term *ethics* in the context of this paper is restricted to the context of computer and information ethics [Bynum 2014]. In this paper we focus especially on the professional responsibility that is expected of system administrators, as encoded by the different codes of ethics in this field. In the field there is consensus that it should have some part in the curriculum, so this is often evaluated by the accreditation committee.

Ethics as part of the curriculum in the System and Network Engineering Master programme was limited to one or two lectures. That is, until 2014 when we started with a new approach. In addition to the lectures on ethics, we force the students to apply their knowledge on ethics. We require students to include an ethical considerations paragraph in all of their project proposals. To support and review this part of the project, we have formed an ethics committee. Since the start of the ethics committee in 2014, we have reviewed over 150 project proposals for eight courses.

In this paper we would like to share our experiences in setting up an ethics committee, the procedures we defined, as well as some example cases of ethical review of student projects. From our experience and as also seen in literature, it is important to share experiences with others. We are sharing this experience so others can learn from our process and experiences, but also about our ethics considerations, so that eventually we may come to a more uniform view.

The rest of this paper is organised as follows: first discussing related work in section 2, then section 3 describes the organisation of the ethics committee. In section 4 we describe several cases as handled by our ethics committee, and finally in section 5 we give our conclusions and some possible future work.

2. RELATED WORK

There is some difference in approach between the US and the EU regarding review of ethics. Universities in the US tend to have an Institutional Review Board[Wikipedia 2015b], which reviews

any research-project which have any kind of involvement from human-subjects. Universities in the EU tend to have an Ethics Committee[Wikipedia 2015a], which generally are focused on medical research, focussing on reviewing research-projects involving human-subjects for clinical trials. The concept of having ethics committees reviewing computer science research-projects is still very new both in the US and EU, yet IRBs in the US are already somewhat more generic and accepted in fields other than medical research, which is not the case in the EU.

The importance of teaching ethics to computer scientists has been identified as early as 1989 [Couger 1989], and has resurfaced later [Dodig-Crnkovic 2004]. Extensive teaching material exists expressly aimed at computer scientists [Baase 2012].

The ETHICOMP conference series has a track on teaching computer ethics since 1995, and many related papers have been presented there, both on experiences in teaching ethics, as well as possible new approaches to ethics. These have been aimed at general computer science curricula, whereas system administration, and especially computer security, requires a different approach.

An extensive ethical review of a research project measuring the effectiveness of the PirateBay blockade has been published by this author [van Wynsberghe and van der Ham 2015]. The nature of this particular research project warranted an extensive ethical review; Bittorrent clients were identified without their permission, in order to measure the impact and effectiveness of a particular website blockade. This research project was performed at the University of Amsterdam, but did not take place in the context of the education programme, and predated both the institutional as well as the Master ethics committees.

The aforementioned CREDS workshops [Bailey and Kenneally 2014b][Bailey and Kenneally 2014a] have discussed different approaches, including the initial development of a model for best-practices [Dietrich et al. 2014]. A followup paper to the two CREDS workshops [Kenneally 2015] provides a good outline of the problems security researchers face, and provides some guidelines on how to deal with them.

This paper does not present a new framework, analysis method, or specific teaching material for teaching and reviewing ethics. In this paper we extend these ideas with a practical and more pervasive application of teaching ethics as part of the complete curriculum, specifically targeted at system administrators and computer security experts. The guidelines and frameworks have been used as input for the way the ethics committee analyses the proposals submitted.

3. ETHICS COMMITTEE ORGANISATION

Ethics as part of the System and Network Engineering Master education has long been a subject that we struggled with. We have attempted to teach students about this during several lectures, where we were able to reach some students, but not all. This was observed by the project proposals that were later submitted by students, which often included unethical subjects or research methodologies. For many subjects in the curriculum we combine abstract and practical approaches to teaching, but we did not apply this to the subject of ethics. This insight, combined with remarks in the 2014 accreditation report and changes in the institutional position regarding ethics prompted us to rethink our approach to teaching ethics. The accreditation committee gave a positive rating to the education, but provided two minor points:

> As two minor points, the panel recommends to address the ethical, societal and social aspects more strongly and to give the business organization aspects a more prominent place. [NVAO 2014]

The change in the position of the university towards ethics actually came about by a student project in the SNE Master; some years ago, students examined the security of a Dutch banking app. In the course of their project they managed to find a vulnerability in the banking app, which made it possible to perform a man-in-the-middle attack. The findings were kept secret initially, and the management of the faculty was alerted, while initiating a responsible disclosure procedure to the bank. Eventually this procedure completed successfully, but along the way the management and legal department of the faculty realised that they were not prepared for this. Combined with

other developments, the faculty formed an ethics committee for the computer science department in 2013, proposing a procedure for handling research proposals. Proposals could be submitted to the committee for review, and the committee would review projects within two weeks.

3.1. Education on Ethical Aspects

The SNE Master programme is an intensive one year program, which include several courses with (research) projects. A timeline of two weeks for approval causes a significant risk for delay in the programme, courses take roughly eight weeks, and projects are usually a subset of those eight weeks. Additionally, the workload of reviewing all student project proposals would be impractical for the institutional ethics committee, there are roughly 30 students in this programme each year, with two courses in each block of eight weeks, this means an average of 30 proposals to review every eight weeks, just for this Master programme.

This prompted us to start an ethics committee for the SNE Master programme. This ethics committee is comprised of three members: the programme director, the security track coordinator, and an ethics advisor. The education of the ethical aspects in the SNE Master is comprised of several parts:

— An introductory lecture, in which ethical theories are introduced, and the evaluation procedure is explained,
— In a course with a (research) project, the students must write a project plan, which must contain a section on ethical considerations,
— The teacher of the course performs a first review of the project proposals, and provides an initial categorisation,
— The SNE ethics committee reviews the categorisation, and creates a final categorisation (within three days after the teachers' review),
— Students receive extra guidance from the ethics advisor appropriate to the categorisation.

3.2. Reviewing Ethical Aspects

Project proposals are put into four different categories:

Green. There is no possibility of ethical issues in this project.
Examples are offline analysis of very specific tools, or projects where no possibility exist to access sensitive data of third parties.
Yellow. There is a small possibility of ethical issues.
Examples are offline analysis of tools or operating systems, where an issue may allow others to gain access to sensitive data.
Orange. There is a real possibility of ethical issues.
Examples are research using personally identifiable information, obtained with prior permission, or sandbox analysis of important secure applications.
Red. There are clear ethical issues in this research.
Examples are research where (for whatever reason) personally identifiable information is obtained without prior permissions, or online analysis of applications involving third parties.

Once the proposals are categorised and approved, the students start with their projects, and a summary of the projects and their categorisation is copied to the institutional ethics committee. The projects are supervised as normal by the teacher and the teaching assistants. Additionally, the students are supervised by the ethics advisor on ethical aspects of their project. This ethical supervision is increased with higher categorised projects. The students are also encouraged to come to the ethics advisor if they find any ethical issues during their research.

Projects that are categorised as *Red* are first discussed in the SNE ethics committee. These projects are normally denied. If the ethics committee sees strong educational or societal value, then the project can be submitted to the institutional ethics committee for approval. The project can only continue if the institutional ethics committee approves the project. Furthermore, should students

disagree with the ethical categorisation of their project, they can also escalate the procedure to the institutional committee.

3.3. Summary of experiences

The ethics committee for the SNE Master education started in 2014, since then the categorisation has been applied to over 150 project proposals, in 8 different courses (including repeated instances of the same course). As mentioned before we feel it is important to share our deliberations on these cases. We feel publishing these deliberations can help start the discussion, so that we can come to a somewhat uniform view on where the boundaries are for ethically acceptable research in system administration.

The students are warned before and during the projects that any issues they may encounter should be brought to the attention of the teacher or ethics committee immediately. This includes new insights into their project which would impact the ethical assessment, but also vulnerabilities discovered. Vulnerabilities will always be kept secret while the project is ongoing. Once sufficient analysis on the vulnerability is completed, a responsible disclosure procedure will be started with the relevant vendor.

Any responsible disclosure procedure is always done in accordance to the guidelines set by the National Cyber Security Centre [Centre 2013]. Summarised this means that any vulnerabilities found will not be exploited any further than to prove their existence and severity, no personal information will be downloaded from the system, nor will a service be disabled. The procedure is always initiated by the university staff, for reasons of responsibility, but also for continuity; these procedures unfortunately take a long time, and may extend well beyond the graduation of the student. For parties that have not published a vulnerability disclosure policy, we contact the party with an initial email describing global details of the vulnerability. In addition, we explain that we act in accordance to the before mentioned Responsible Disclosure-guidelines, request a statement that the company will not prosecute, and also set an initial, negotiable deadline for addressing the vulnerability.

4. CASE DESCRIPTIONS

This section contains descriptions of several cases that have been categorised by the SNE Master ethics committee. The examples given below are a selection of projects from the courses Offensive Technologies and Research Projects[1]. These examples were selected for illustrative value and diversity, other courses follow the same requirements and approach. The full reports of these cases are also available[2].

As mentioned before our approach for evaluation ethical considerations in student projects is inspired by the framework as described in [Dietrich et al. 2014]. We have extended that framework beyond the considerations of data sharing. An important aspect is the possible discovery of vulnerabilities in products, and their impact towards different groups: the vendor, the users, and the general public. We attempt to identify and balance all these factors when categorising the student research projects.

In some of the projects, the ethics advisor has suggested changes in the way that experiments were conducted, or how data was gathered. The advisor and the teaching assistants try to keep an eye on the students and their actions during the project. Since this is a Master level education, we do expect a certain degree of independence and responsibility from the students. We also instruct the students that the ethics committee is there for their protection; if they act within the bounds as defined by the ethics committee and advisor, the university will try to protect them as much as possible.

4.1. Project: Tinder Stalking

[1] See https://www.os3.nl/2015-2016/info/curriculum
[2] See http://staff.fnwi.uva.nl/j.j.vanderham/cases/

4.1.1. Project Summary. Tinder is a popular dating app, which allows users to discover other nearby users. This process of course depends on providing location data, which historically has not been properly protected by Tinder [Veytsman 2014]. Tinder uses information from Facebook profiles, for example the pictures used in the matching process are taken from there, and users are provided with an indication of overlapping interests from their Facebook profiles. In this research project the students attempted to verify whether Tinder had successfully implemented additional measures to secure the location data, and wanted to investigate whether it was possible to link Tinder users back to their Facebook profile.

4.1.2. Ethical Analysis. There is a clear risk in this project for obtaining information without informed consent from the participants. Due to the nature of this service, it was not possible to perform this research offline. Another important consideration in evaluating this proposal was that Tinder had been warned about possible problems multiple times in the past, and each time attempted to solve the problem. Initial approval for this project was given with the restriction that experiments would only be performed with either test profiles or profiles of their classmates with informed consent. With that restriction, and because Tinder had been repeatedly warned about this issue, the project was classified as *Orange*.

The students were able to query the server for nearby users, and a limited list of candidates would be returned. The approach required repeated query-results with different parameters for the same identifier. During the execution of the project the students discovered that due to the popularity of Tinder, it was hard to work with a limited set of profiles.

After discussion with the ethics advisor the experimental design was changed so that only a limited set of information from the query-results was used. Instead of looking for a single profile identifier, the students stored the location data, combined with a hash of the account identifier. This made it possible to perform the experiment, while maintaining the anonymity of Tinder users. The data would also be destroyed at the end of the project.

4.1.3. Outcome. During the project the students discovered that they were able to track location of Tinder users. As mentioned above, the methodology was designed to prove this result while preserving the anonymity of Tinder users. The students also found that (manually) using Facebook Graph search they could discover the profile of Tinder users, with high probability.

The staff attempted to initiate a responsible disclosure procedure with Tinder early 2014 several times, through several different contacts. Eventually the initial message was acknowledged, promising a response. After three months of no response, the staff decided to publish the report. As far as is known, it is still possible to track Tinder users using this method.

4.2. Exploiting Wireless Networking Memory Cards

4.2.1. Project Summary. Wireless networking memory cards are like regular SD memory cards. They provide access to a camera to store pictures, but at the same time a small System-on-a-Chip provides wireless networking capabilities, over which the files on the storage medium can be accessed. This provides a way wirelessly transmit pictures from cameras that do not have wireless networking capabilities. The students in this research project tested the security of the wireless networking implementation.

4.2.2. Ethical Analysis. Before this project no similar research on the security of these kinds of memory cards had been performed. Due to the limited capabilities of the implementation there was a significant possibility that the students would find vulnerabilities in this implementation. If found, these vulnerabilities would have far reaching effects on the viability of the products. The project would be performed in a lab environment, on prepared cards, to minimise the impact of finding a possible vulnerabilities. This project was classified as *Yellow*

4.2.3. Outcome. The students were able to identify multiple vulnerabilities in the different memory cards. They were able to reverse engineer the key generation process, for both the network and the access restriction on the card. Responsible disclosure processes were started with the manufac-

turers, and both responded. One manufacturer researched the vulnerability, acknowledged it, while pointing out that there was a mitigation strategy available for users. They were considering improvements in future products. The other manufacturer acknowledged the report, but did not seem to escalate the issue beyond the support desk.

4.3. Drone Hijacking

4.3.1. Project Summary. Communication with flying drones is mostly over some form of wireless networking. Most commercially available drones use simple networking that is often not secured very strongly, because of limited processing power and cost issues. Drones used for law enforcement should however have secure wireless networking. In this project the students examined the wireless communication used in drones that are similar to the ones used by law enforcement.

4.3.2. Ethical Analysis. Disturbing traffic to drones, and especially to those used by law enforcement agencies can be dangerous. While the experiments and analysis would be done completely offline, there is a possibility that vulnerabilities would be discovered during the project. Vulnerabilities in these products would have a severe impact, especially if they would become public. The project was conducted in cooperation with a drone manufacturer. This project was classified as *Orange*

4.3.3. Outcome. The students were able to record and analyse the communication between the drone and the remote. The video feed on the drone was actually transmitted over wifi, with weak security and default password. The control of the drone was sent over a separate channel. The students were not able to gain complete control over the drone, but they were able to use a replay attack on some commands, such as 'start and lift off', which starts the engine and lets the drone hover a few centimetres above the ground. These vulnerabilities were reported to the vendor, who acted on them quickly.

4.4. Peeling the Google Public DNS Onion

4.4.1. Project Summary. Since several years, Google provides a public DNS resolving service at the IP addresses `8.8.8.8` and `8.8.4.4`. Google published [Google 2015] that these resolvers are located in over a dozen different countries around the globe, but no information on the inner working of the resolving system is known. In this project the students tried to investigate the inner working of this service, and especially the cache distribution and the different cache levels within the service. The RIPE Atlas [RIPE NCC 2014] platform was used as a measurement platform. This allowed the students to use many different probes to submit queries to the Google DNS service in a geographically distributed manner.

4.4.2. Ethical Analysis. The project aims to analyse the public DNS service using public information, and regular queries to the Google DNS service. The number of queries was considered briefly, but this was quickly deemed negligible relative to the normal number of queries that are submitted to this service. The RIPE Atlas measurement platform uses credits for measurements, daily limits for each user, as well as global limits for each measurement target, to make sure that the measurement system is not abused. This project was classified as *Green*.

4.4.3. Outcome. The students used specifically created DNS zones and individually created measurements in the RIPE Atlas platform. During the project they discovered that the limits put in place in the Atlas measurement system restricted them from performing the research. After contact with the RIPE Atlas engineers, the usage limit for the students was increased temporarily for the duration of the project. Towards the end of the project, the students also contacted the Google DNS team to verify their findings. The team was cooperative, and confirmed some of their findings.

4.5. Evil SSD

4.5.1. Project Summary. The NSA had a programme called IRATEMONK [Schneier 2014], which uses a hard drive firmware to gain persistent access to a target computer. The NSA apparently

used this exploit already since 2008. In this project the students researched the feasibility of hiding malicious code in SSD hard drive firmware, as well as the possible capabilities of malicious code in that firmware. For this project the students would be provided with a new SSD on which they could use an open source firmware, that they could adapt to test the possibilities and capabilities.

4.5.2. Ethical Analysis. The materials used for this project were all provided especially for this project, with no personal data on them. The students would perform their experiments in a controlled environment, without any external users. Any possible results would be published publicly, they do not concern a specific manufacturer of SSDs. In the project the students would try to adapt an open-source firmware for SSD drives[at Sungkyunkwan University 2015]. This firmware is meant for an SSD development platform, can only be used on specific older SSD models, and does not provide complete functionality (i.e. modifications of the drive contents are lost after rebooting).

There was a serious possibility that students would find significant capabilities for backdoors or hiding data, which can be used for malicious activities, however, any vulnerability would only work on this specific firmware. The research project and the published results would help the security community gain more understanding of what is possible with these kinds of advanced implants. With all this in mind, the project was classified as *Green*.

4.5.3. Outcome. The students were able to successfully implement a backdoor in the open source firmware. This backdoor is capable of modifying data as it is retrieved from the drive, presenting for example additional password hashes, or replacing complete binaries. This firmware however can only be used in one (old) specific type of SSD, and even then is not able to perform persistent writes.

4.6. RFID Lock Security Assessment

4.6.1. Project Summary. In the course of the study, students become more observant of possible security problems. One student observed that in a particular student housing, RFID locks were used throughout the building: both for entry to the main building as well as the personal dorm rooms. Tenants receive a personal RFID card which allows them to access their personal dorm room. It was already known that these RFID cards were not well protected, as it easily possible to read and copy the RFID cards. The student also observed that the locks in this building could be updated wirelessly, for example for a new tenant of a dorm room. In this project the students proposed to research the security of these wireless updating mechanisms.

4.6.2. Ethical Analysis. In the first proposal the students would be attempting the assessment at the dorm, which would mean that they would perform the observations on a live system. They would be attempting to capture and possibly replay radio signals in this live environment, possibly interfering with the security of systems outside of their control. This was categorised as *Red* and denied by the ethics committee.

After discussion, the ethics committee proposed that the student contact the owner of the dorm, to seek permission. Another option was to contact the manufacturer of the RFID locks to obtain testing equipment, so that the assessment could be performed offline. The student received negative answers from both the owner, as well as the manufacturer of the RFID locks. This meant that the project could not be performed within the context of the educational programme.

5. CONCLUSION

Ethics is an important part of education in system administration. It is a hard subject to teach to students who are used to exact sciences, yet it touches almost everything that they do. In this paper we have described our new approach to teaching ethics in the context of the System and Network Engineering Master education of the University of Amsterdam.

As a first step we have introduced an ethics committee to review student project proposals on their ethical aspects. In the project proposal the student writes an ethical considerations paragraph describing the possible issues relevant to the proposed research. This is to facilitate the committee, but also to reenforce the learning and applicability of ethics to the students. The projects are then

categorised according to the possible risks and ethical issues that the students may encounter during the execution of the project. The intensity of guidance by the ethics advisor that the students receive depends on this categorisation.

In the second part of this paper we have described six different cases that have been evaluated by the ethics committee, with outcomes in several different categories. These project descriptions illustrate that ethical issues in education of system administration are numerous and diverse. They can range from privacy of users of external services, products, or software, but even to physical security, with drone communication and RFID locking systems. With these case descriptions we hope to engage with other ethics committees and other researchers to discuss ethical aspects of security research.

The experiences in reporting vulnerabilities were varied. Any vulnerabilities found by students are always reported to organisations using responsible disclosure procedures. Some organisations have ignored the reports, sometimes not even acknowledging receiving the report. This unfortunately means that setting initial deadlines is necessary. Most organisations though are grateful for the reports, acknowledge the issues and either act on them, or found the issues not serious enough to warrant action.

We have not received negative responses on our reports, besides the organisation not granting permission. It should be noted that disclosure procedures often take a long time. With small issues and cooperative organisations, they can be resolved within a day, but other issues can drag on for much longer. In one case we cooperated with a company to fix a vulnerability in their application, and the whole procedure took several months before it was finally resolved and published.

The experiences so far with the ethics committee have been positive. With the previous approach on ethics using lectures, the subject remained abstract and distant, even when discussing concrete examples. With the new approach, writing the ethical considerations paragraph forces the students to think about the issues, which leads to more open discussions, both with the staff, but also between students. The subject now also lives on through the whole programme, instead of only concentrated in the lectures.

An important consequence from starting our ethics committee is that it has increased internal support for the security research that the students are doing. With the committee we demonstrate that we have identified sensitive issues in the students research projects, and are capable of monitoring them.

Interest in computer ethics has increased, in society due to the pervasiveness of computers, and the practices of businesses and intelligence services. The field itself has also realised that ethics is an important issue to keep in mind, as big data experiments give rise to surprising privacy invasions, and vulnerabilities in software can have a serious impact on people or even society. The field of computer security should consider self-imposed regulation for reviewing ethics, before a more strict regulation is imposed by outsiders.

5.1. Future Work

With this paper we have demonstrated how we approach ethical analysis of student research projects. We are interested in hearing how other educational programmes in this field are handling similar issues. The case descriptions can hopefully help with a constructive debate, and perhaps as training material for similar committees.

For the analyses of the projects we roughly follow the general framework [Dietrich et al. 2014], in the future we would like to further fine-tune this framework to fit with the educational context of this field.

ACKNOWLEDGMENTS

The author would like to thank Jaap van Ginkel and Karst Koymans, the other members of the Ethics Committee, for their support and constructive discussion on these and other cases.

REFERENCES

Computer Systems Laboratory at Sungkyunkwan University. 2015. The OpenSSD Project. (2015). Retrieved 9 Septemeber 2015 from http://www.openssd-project.org/wiki/The_OpenSSD_Project

S Baase. 2012. *A Gift of Fire: Social, Legal, and Ethical Issues for Computers and Internet*. Prentice Hall, Upper Saddle River, New Jersey.

M. Bailey and E. Kenneally. 2014a. Cyber-security Research Ethics Dialogue & Strategy (CREDS) Workshop, CREDS II - The Sequel . (2014). Retrieved 28 July 2015 from http://www.caida.org/workshops/creds/1405/

M. Bailey and E. Kenneally. 2014b. Cyber-security Research Ethics Dialogue & Strategy (CREDS) Workshop Report. *ACM SIGCOMM Computer Communication Review (CCR)* 44, 2 (Apr 2014), 76–79.

Terrell Bynum. 2014. Computer and Information Ethics. In *The Stanford Encyclopedia of Philosophy* (winter 2014 ed.), Edward N. Zalta (Ed.).

National Cyber Security Centre. 2013. Responsible Disclosure Guideline. (2013). Retrieved 29 July 2015 from https://www.ncsc.nl/english/current-topics/responsible-disclosure-guideline.html

SAGE Executive Committee. 2003. System Administrators' Code of Ethics. (2003). Retrieved 27 July 2015 from https://www.usenix.org/lisa/system-administrators-code-ethics

J Daniel Couger. 1989. Preparing IS students to deal with ethical issues. *Mis Quarterly* (1989), 211–218.

ACM council. 1992. ACM Code of Ethics and Professional Conduct. (1992). Retrieved 27 July 2015 from https://www.acm.org/about/code-of-ethics

Sven Dietrich, Jeroen Van Der Ham, Aiko Pras, Roland van Rijswijk Deij, Darren Shou, Anna Sperotto, Aimee Van Wynsberghe, and Lenore D Zuck. 2014. Ethics in data sharing: developing a model for best practice. In *2014 IEEE Security and Privacy Workshops (SPW)*. IEEE, 5–9.

Gordana Dodig-Crnkovic. 2004. On the importance of teaching professional ethics to computer science students. In *Computing and Philosophy Conference, E-CAP*. Citeseer.

Google. 2015. Google Developers: Public DNS. (2015). Retrieved 30 July 2015 from https://developers.google.com/speed/public-dns/

Erin Kenneally. 2015. How to throw the race to the bottom: revisiting signals for ethical and legal research using online data. *ACM SIGCAS Computers and Society* 45, 1 (2015), 4–10.

NVAO. 2014. Assessment report Master System and Network Engineering, University of Amsterdam. (2014). https://search.nvao.net/files/53da2b8c1ff3d_rapport%20UvA%20wo-ma%20System%20and%20Network%20Engineering.pdf

RIPE NCC. 2014. RIPE Atlas. (2014). Retrieved 30 July 2015 from https://atlas.ripe.net/

B. Schneier. 2014. IRATEMONK: NSA Exploit of the Day. (2014). Retrieved 31 July 2015 from https://www.schneier.com/blog/archives/2014/01/iratemonk_nsa_e.html

Aimee van Wynsberghe and Jeroen van der Ham. 2015. Ethical considerations of using information obtained from online file sharing sites. *Journal of Information, Communication and Ethics in Society* 13, 3/4 (2015), 256–267. DOI: http://dx.doi.org/10.1108/JICES-10-2014-0044

Max Veytsman. 2014. How I was able to track the location of any Tinder user. (2014). Retrieved 28 July 2015 from http://blog.includesecurity.com/2014/02/how-i-was-able-to-track-location-of-any.html

Wikipedia. 2015a. Ethics Committee. (2015). Retrieved 9 September 2015 from https://en.wikipedia.org/wiki/Ethics_committee_(European_Union)

Wikipedia. 2015b. Institutional Review Board. (2015). Retrieved 9 September 2015 from https://en.wikipedia.org/wiki/Institutional_review_board