

Seminar:  
The Computer Engineer's Code of Ethics

Daniel Bosk\*

ethics.tex 2169 2015-01-14 22:37:01Z danbos

## Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Aims</b>	<b>2</b>
<b>3</b>	<b>Theory</b>	<b>2</b>
<b>4</b>	<b>Assignment</b>	<b>2</b>
<b>5</b>	<b>Examination</b>	<b>3</b>

## 1 Introduction

Considering that our world becomes increasingly dependent on computer systems, it is important that those of us who are capable of controlling the computer systems do this in a responsible way. But what is a responsible way? This is the topic of ethics, the reasoning about moral obligations. There are a great many texts written on the subject, we will in this assignment study some of the lighter ones.

As an example, since our digital world allows the copying of information more easily, more people do this. This can happen in the form of people using a service for publishing photographs to friends, or to the entire world for that matter. Sometimes the consequences of this can be severe. For instance, when a child posted vacation pictures to Instagram [1]. This happened to be not any child, it was the child in the Norwegian royal family. These images posted, did due to our technical development, contain the exact GPS coordinates of the location where the picture was taken. The result being that the position of the royal family was published in almost real-time, information which is normally strictly secret.

---

\*This work is licensed under the Creative Commons Attribution-ShareAlike 3.0 Unported license. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/>.

This is also an issue for non-celebrities. And the question is, where ends the responsibility of the engineers who contributed to these systems? Should they be morally obliged to ensure the user can make an informed choice? Or is that totally the responsibility of the user?

We can then step it up a notch. In app stores, e.g. Google Play, there are occasionally apps found which performs some morally questionable activities. An Android app, “Brightest Flashlight” by Goldenshores Technologies, which could be found for free in the Play store, gathered data on users’ locations and device identifiers, which the company later sold to advertisers [2].

Another, more draconian, example concerns manufacturers of surveillance equipment, selling this equipment to authoritarian regimes for purposes of surveiling, censoring and in general repressing the people, as is the case for the companies Narus, BlueCoat Systems, Trovicor and Cisco [3]. Narus sold equipment used for surveillance to the Egyptian government. BlueCoat’s equipment was used in Syria. Germany-based Trovicor sold their technology to Bahrain; “dozens of activists were tortured before and after being shown transcripts of their text messages and phone conversations captured from this technology” [3].

Is this type of engineering anywhere near ethically defensible?

## 2 Aims

This seminar aims to discuss the ethical issues regarding the problems described above, i.e. the moral responsibility of engineers. After doing this assignment you should be able to:

- Value and argue about different ethical aspects of computer security, e.g. possibilities for surveillance, and its consequences in society.

## 3 Theory

This assignment is based on the Codes of Ethics of two engineering associations. Thus, before you start you must read “Code of Ethics” [4], “Software Engineering Code of Ethics and Professional Practice” [5], and finally “IEEE Code of Ethics” [6].

Once you have read this you should read two articles analysing Snowden’s revelations about the NSA surveillance techniques. The first one is “Making Sense from Snowden” [7]. The second one is “Highlight from Making Sense of Snowden, Part II” [8].

Finally, in your favourite search engine, search for the string

“nsa exploit of the day site:www.schneier.com”.

Read about a few of the NSA exploits presented there.

## 4 Assignment

You are now going to position yourself as one of the engineers working for the NSA, one of those who contributed to the exploits the NSA uses to collect information.

Prepare a document with two parts. The first part should contain arguments for why you should develop these exploits, the second should contain arguments against developing these.

Your arguments should have their base in the Codes of Ethics you have read (include references), but also other ethical values may be used in your argumentation. Also, to make your argumentation more clear, use some of the actual exploits, their use and possible consequences as examples for your argumentation.

## 5 Examination

This assignment is examined through active participation in a seminar and a hand-in. To prepare for this seminar you must write your two documents mentioned above. You hand these in in the course platform, they must be in PDF format. Then you attend the seminar, see the schedule. You must participate actively to pass this assignment.

## References

- [1] Paul Roberts. *Wayward Instagram account creates security scare for Norwegian Royal family*. Aug. 2012. URL: <http://nakedsecurity.sophos.com/2012/08/23/instagram-norway-royals/>.
- [2] Lee Garber. “Security, Privacy, Policy, and Dependability Roundup”. In: *IEEE Security & Privacy* 12.1 (2014), pp. 9–10. ISSN: 1540-7993. DOI: <http://dx.doi.org/10.1109/MSP.2014.13>.
- [3] Electronic Frontier Foundation. *Mass Surveillance Technologies*. Accessed 4 April 2014. URL: <https://www.eff.org/issues/mass-surveillance-technologies>.
- [4] Association for Computing Machinery. *Code of Ethics: ACM Code of Ethics and Professional Conduct*. Accessed on 4 April 2014. URL: <https://www.acm.org/about/code-of-ethics>.
- [5] Association for Computing Machinery. *Software Engineering Code of Ethics and Professional Practice*. Accessed on 4 April 2014. URL: <https://www.acm.org/about/se-code>.
- [6] Institute of Electrical and Electronics Engineers. *IEEE Code of Ethics*. Accessed on 4 April 2014. URL: <http://www.ieee.org/about/corporate/governance/p7-8.html>.
- [7] Susan Landau. “Making Sense from Snowden: What’s Significant in the NSA Surveillance Revelations”. In: *IEEE Security & Privacy* 11.4 (2013), pp. 54–63. ISSN: 1540-7993. DOI: <http://dx.doi.org/10.1109/MSP.2013.90>.
- [8] Susan Landau. “Highlights from Making Sense of Snowden, Part II: What’s Significant in the NSA Revelations”. In: *IEEE Security & Privacy* 12.1 (2014), pp. 62–64. ISSN: 1540-7993. DOI: <http://dx.doi.org/10.1109/MSP.2013.161>.