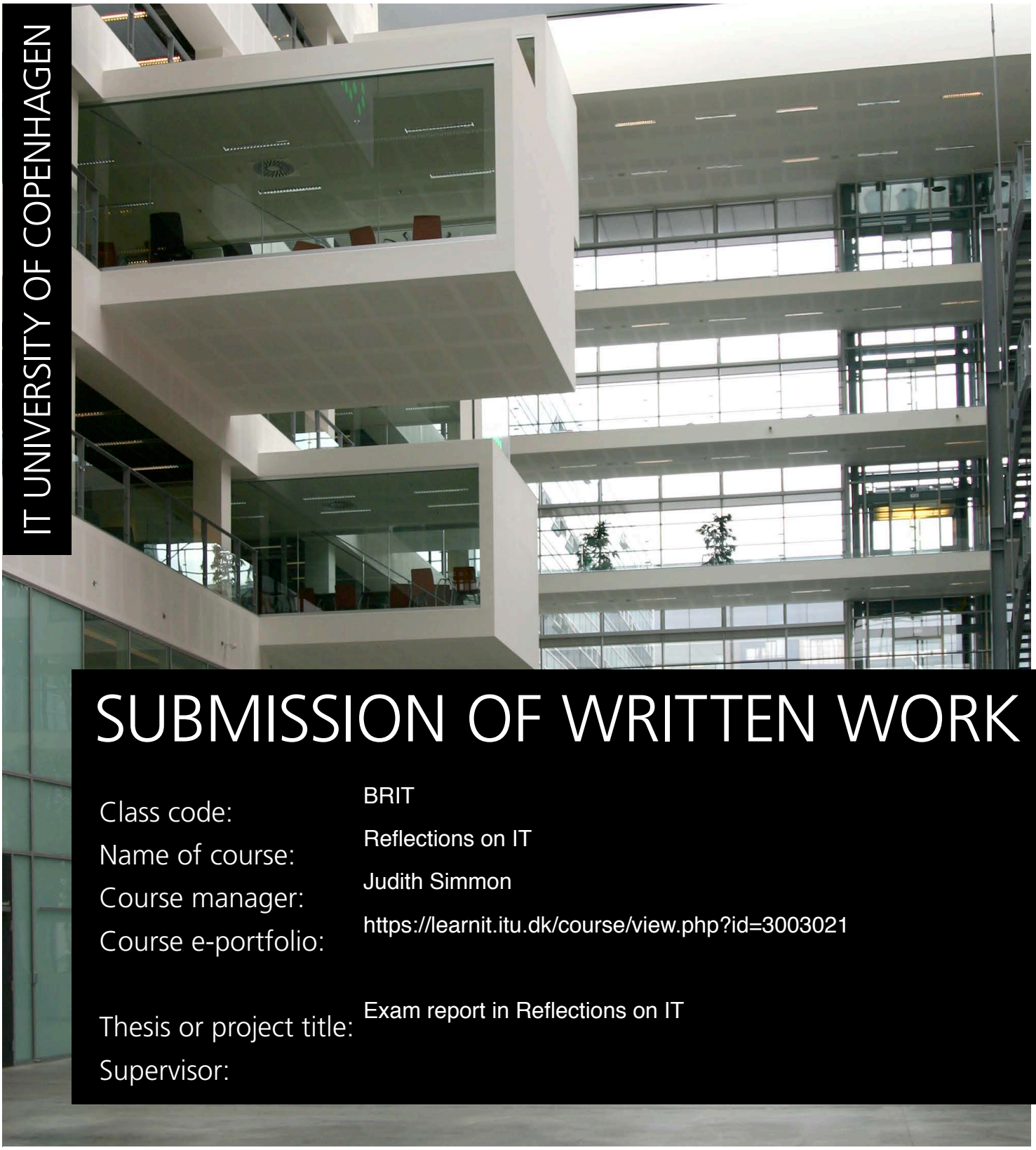
IT UNIVERSITY OF COPENHAGEN



SUBMISSION OF WRITTEN WORK

Class code:	BRIT
Name of course:	Reflections on IT
Course manager:	Judith Simmon
Course e-portfolio:	https://learnit.itu.dk/course/view.php?id=3003021
Thesis or project title:	Exam report in Reflections on IT
Supervisor:	

Full Name:	Birthdate (dd/mm-yyyy):	E-mail:
1. Nikolaj Zangenberg Lollike	12/06-1992	nlol@itu.dk
2.		@itu.dk
3.		@itu.dk
4.		@itu.dk
5.		@itu.dk
6.		@itu.dk
7.		@itu.dk

Exam paper in Reflections on IT: The societal impact of decentralised computing

Nikolaj Zangenberg Lollike - nlol@itu.dk

September 1, 2015

Contents

1 Introduction

In this paper, I will discuss the societal impact of *decentralisation of computing*, a new paradigm in computing that was sparked by the introduction of *Bitcoin* in 2009, by being the first big decentralised autonomous organisation (from here on *DAO*). New technologies inspired by Bitcoin, such as *Ethereum*[1], have taken this technology of monetary transactions further and implemented a generic block chain technology that allows for any kind of transaction, essentially laying the ground work for what they call *Web 3.0*, a decentralised web where applications and corporations will be run decentralised[1]. To use their layman explanation:

> It's a really, really big computer made of many computers around the world that check each other's results, and where everyone can run programs on, paying only for what they use[2].

This technology could be the start of a free and completely transparent and open internet, with completely anonymity for those who want it. This however could also spark more criminal activity in the form of black market sites like *Silk Road*, an online drug selling forum, that was shut down by the FBI on the 6th of November 2014[3]. And maybe even more concerning this could allow for terrorist networks to communicate and avoid surveillance. Will decentralisation shift the power from big corporations and governments to the users? And how will this new landscape impact ethical topis like surveillance, privacy and censorship of users? To find out I will analyse the current landscape in order to discuss how this paradigm-shift in computing might impact society.

[1] http://ethereum.org

[2] http://www.quora.com/Ethereum/What-is-Ethereum-in-laymans-term

2 The current landscape

2.1 Private centralised corporations owns your data

Today, most software and its data are centralised. Applications and its data are run on centralised web servers – more specifically on a specific computer in a specific location owned by a specific corporation. On top of that, this corporation essentially owns all the data you create using their service.[7]

Take for example social media. Services like Facebook, Twitter and Instagram are used by virtually everyone and generates immense amounts of personal data[15]. Normal users will not have an understanding of computing and what "goes on under the hood" of such web services, due to what Moor calls the *invisibility factor*[10]. He argues that a user has a good understanding of what goes in the computer and what consequently comes out, but very limited knowledge of the internal processing. It all boils down to the fact that the user cannot investigate the internal operations, so certain surveilling or even malicious software can be hidden. In the case that a corporation is law-abiding and not intentionally hiding surveilling applications in their software, the only way to get knowledge of this is through reading the *Terms and Conditions* – the document that describes the contract between the user and the services.

The problem though is that these documents are usually written in a legal language with a huge amount of information in very little space, making it extremely difficult for layman to follow[8]. This results in a very low grade of transparency and consequently the user has no idea of what rights he has and what terms he agreed to. This is something we are all acostumed to – the documents are simply too long and too cumbersome that no one reads them[13]. And we have simply accepted that it is how it is.

2.2 The government is spying on you

However more problematic is how government taps into this data with no trace and no statements that this is in fact happening. Time and time again stories surface that the *National Security Agency* (from here on NSA) is

tapping into users private data, without the users knowing[6]. In these cases there no transparency at all. They defend their actions by arguing that it is to combat terrorism and ultimately for the security of citizens[4]. I think it is safe to say that in today's world virtually everyone using big online services of any kind are under some sort of government surveillance. But how much this is the case and the methods these agencies use are very much engulfed in secrecy as Glenn Grenwald points out[5].

2.3 Censorship

Since 2005 Denmark has been censoring certain content on the internet[14]. Almost all danish internet service providers has a filter that blocks unwanted websites regardless of whether the user wants it or not. This filter was put in place in order to combat child pornography, but the censorship has since spread to block streaming, gambling and torrent sites such as *The Pirate Bay*.[3] Not only is this censorship a grey-area in terms of section 77 in the Danish constitution that states:

> Enhver er berettiget til på tryk, i skrift og tale at offentliggøre sine tanker, dog under ansvar for domstolene. Censur og andre forebyggende forholdsregler kan ingensinde på ny indføres[4].

To translate briefly it says that *"everyone has the right to express themselves publicly and freely. Censorship or preventive measures shall never be installed again"*. The actions of today's government are thus in violation of this since they are in fact implementing preventive measures.

2.4 Decentralising our way to a free and open internet

The new paradigm of decentralisation of the internet would dramatically change this current landscape. All operations would be transparent and secure. No one would be able to censor or tamper with data without the

[3]A list of DNS blocked websites in Denmark: `http://www.teleindu.dk/wp-content/uploads/2013/01/Oversigt-over-DNS-blokeringer-28-10-2013.pdf`

[4]The danish constitution: `http://www.grundloven.dk/`

public knowing. And you can be sure that NSA is not listening to your conversations. Your identity can be anonymous, and your privacy intact. Seemingly this would be a more free society – but would it be ethical right? In order to discuss this I will dive into the topics I have already outlined in this paper.

Is it ethical that companies own your personal data? Is it ethical right to have a very low grade of transparency of what happens to this data? Is it the users responsibility to be informed of what they are doing online, or does corporations have a responsibility in informing the users? Is it ethically right for government to offer no transparency of what surveillance is going on, now that companies are forced to obey certain laws and inform the users through Terms and Conditions? Is it ethical right to surveil citizens in order to protect them?

2.5 Ethics in the global society

As you can see above, we face some ethical questions regarding computer technology. Due its borderless, seemingly unlimited nature it is hard to apply the existing rules of society. The internet is a global society, but the ones who are part of it come from many different societies, with different laws and concepts of freedom and privacy. Who are the ones to issues the laws and rules there? How do we determine right and wrong in such a society? This revolutionary technology needs a new set of ethical rules in order to deal with these ethical questions in a meaningful way. Wiener and Moor have tried to define *computer ethics* and I will investigate their definitions and methodology of solving information technology related ethical questions in the following section.

3 Theory

So what are computer ethics anyway? How do we deal with complex questions like the former?

3.1 Wiener's computer ethics

Norbert Wiener laid the foundation of computer technology ethics by defining the science he called *cybernetics*[2]. Bynum's interpretation of Wiener's thoughts is that the science was in fact the start of computer ethics. Bynum states[2]:

> According to Wiener, for human beings to flourish they must be free to engage in creative and flexible actions and thereby maximize their full potential as intelligent, decision-making beings in charge of their own lives. This is the purpose of a human life.

Thus freedom is the central key to live fully as a human being, as limitations in freedom means you are not free to make your own decisions regarding what you want to purse in life. If you are not free to make use of a certain talent and fulfil your own potential you are not in charge of your own life. This definition of the purpose of human life led to Wiener's *great principles of justice*, which is 4 principles Wiener thinks society should be based upon. Bynum has named these principles which are as follows:

- **The Principle of Freedom**

  > Justice requires "the liberty of each human being to develop in his freedom the full measure of the human possibilities embodied in him[2]."

- **The Principle of Equality**

  > Justice requires "the equality by which what is just for A and B remains just when the positions of A and B are interchanged[2]."

- **The Principle of Benevolence**

  > Justice requires "a good will between man and man that knows no limits short of those of humanity itself[2]."

- **The Principle of Minimum Infringement of Freedom**

  > What compulsion the very existence of the community and the state may demand must be exercised in such a way as to produce no unnecessary infringement of freedom[2].

As stated above, freedom is central in order for one to have the possibility to develop ones full potential. For everyone to flourish freedom must be equal. And how do we ensure this? By having a society where equality and freedom is accepted, which is this good will between citizens. Therefore society is key because in these principles of justice because it affects every one of them. Bynum proves this by arguing that a despotic society would indeed violate all these principles, why there's need of the fourth principle of *minimum infringement of freedom*.

The methodology of applying these principles is first to identify an ethical question of the implication of computer technology in our society. In order to take an educated stand on the matter, one must be informed on the specific case. Then you try to apply exsiting ethical principles or laws of society. If the case is so revoultionary that this does not suffice you use Wiener's definition of the purpose of human life and principles of justice in conjunction.

3.2 Moor's computer ethics

James H. Moor argues that ethical problems arise in the field of computer technology because there is a *policy vacuum* and *conceptual vacuum* due to its revolutionary capabilities, that gives us entirely new options in life[10]. Basically the technology is so new and evolves so quickly that our laws of society simply cannot keep up with it. So in order to deal with these ethical problems Moor lays down some definitions of what makes computer ethics so special. Moor talks about an *invisibility factor* that can be split into three types of ethical significant topics in computer technology. They are as follows[10]:

- *Invisible abuse* – The case of theft, surveillance or violation of privacy.

- *Invisible programming values* – The case of biased computing, that will lead to a certain outcome.
- *Invisible complex calculations* – The case of humans having to trust super computations that they do not understand.

These invisible factors are key in computer technology, and therefore computer ethics. I will in the following use Wiener's and Moor's computer ethics in order to analyse the current landscape of ethical grey areas I laid out in the beginning.

4 Analysis

Now that we have the theory in place to discuss computer ethics I will analyse the ethical cases decentralisation will influence in order to later discuss the ramifications of this paradigm-shift.

4.1 Intransparency in corporations

In the case of corporations such as Facebook using your data, such as your photos and location[9] we have an issue of transparency. According to Moor this would be a case of invisible abuse because we do not know the inner workings of Facebook and how much we are being surveilled. Facebook's terms of service declare that

> you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License)[5]

This covers what you actively post on Facebook. You could argue that it makes perfect sense that because Facebook owns the web servers that the user is actively putting files and data on, Facebook has some right to this content. However, because I download an illegal mp3 file, do I own the music? I own the physical hard drive, but I do not own the digital rights of the bytes stored

[5]https://www.facebook.com/terms

on this spinning disc. This is an abstract concept that exemplifies why we need computer ethics. Because computer technology stretches the physical limits as we know them into a virtual world. Facebook is transparent about them having rights of the content you post on their site, but they are very intransparent in which use cases they will do so, which would classify as a violation of *the principle of benevolence*.

What Facebook fail to mention in their Terms of Service is how they keep track of which other websites you visit using cookies[9]. This is an example of invisible abuse. To link this with Wiener's principles of justice, this would be an infringement in freedom since Facebook actively track your presence online in order to form an individual reality just for you based on your searches and movement around the web, as ads for example are actively selected to fit you. It would also classify as a bias in computing defined as *invisible programming values* by Moor, thus being unethical.

4.2 Government surveillance

However an even greater example of invisible abuse is when government programs like NSA's *PRISM* program taps into this data of Facebook in order to surveil the public[6]. There is no transparency at all in this process. There is no terms of service that declare that the government is listening in on your Facebook conversations. Even when you search for the PRISM program there is only leaked information. The government surveillance programs are thus kept secretive and no one really knows to what extent this surveillance is going on.

The argument that is used to deem this surveillance ethical is that if you are doing something you do not want anyone to see, you should not be doing it in the first place. Glen Greenwald however rebutes this by arguing how contradicting it is that government themselves hide their actions from public view and that their agencies operate behind a wall of secrecy so big that no one really know the size of these organs[5]. He claims that privacy is a central part of being human as we are free to act the way we want in our privacy, thus making it a question of infringing upon human freedom. He

even draws parallels to American constitution, that states everyone has the right to be left alone[5]. All the principles of justice are violated in the sense that freedom and equality are infringed, why this surveillance on this basis is unethical.

4.3 Censorship

In the case of censorship we do not need to apply computer ethics. There are already general ethical rulesets and laws that determine that censorship is unethical. As metioned earlier, the Danish constitution has a section against censorship. This is however also arguable by applying Wiener's definition of the purpose of human life, is to be "free to engage in creative and flexible actions"[2]. Censorship would be a direct violation of all 4 principles of justice. It would obviously be a violation of freedom and equality – since censorship would mean someone having the power to determine what is freely to be expressed while others are not. Censorship would too violate *The Principle of Benevolence* because censorship is the opposite of having good will between citizens of society, thus violating all the principles. Wiener's theory suggest that censorship would be deeply unethical.

However, as stated earlier, there is already internet censorship going on in Denmark for example. You could argue there's an invisibility factor in users just not being able to go to certain sites because of a DNS block. This could be seen as a bias in computing, where some websites are white listed and some are not. This too is unethical according to Moor.

5 Discussion

So is decentralisation the solution to all these problems? Why are these things happening if they are unethical?

5.1 Surveillance

In the case of surveillance, government legitimatise their actions as for protecting the state against criminals who are also trying to infringe upon the

freedom of citizens. That being terrorists who plots attacks or hackers who try to empty your bank account.

We are already surveilled in public, this surveillance however is much more transparent in its nature than the one happening through your electronic devices. You are much more aware of cameras at train stations or of police patrolling the city. They give you a certain sense of security. A security that is also needed to feel capable of acting freely. But there is a big difference in how you act when you are out in the public and at home. When you are at home using your computer, you are in your private sphere. You are already secure, so you do not need the society to keep you safe. However you are in fact in touch with a global society. The surveillance this time though is happening right in your private sphere: your home. And you are unaware how exactly. It can thus be argued that this is indeed an infringement of privacy and freedom. However these security measures are also there to keep us safe. They do not immediately affect us. Most people do not even know about it. So how is it harmful, if you do not even know if you are being surveilled? There is a definite ethical problem in the fact that these agencies are hidden in the shadows and their methods kept secret. It is against democracy that government does not inform the public of its operations in some form, granted that the program needs to be somewhat secret in order to work. But the scale of surveillance by the NSA was kept secret for many years before it was eventually leaked by Edward Snowden.

Decentralisation in the form that Ethereum suggest would mean that all operations would be public, and thus you would be able to see whether or not you were being surveilled[1]. The invisibility factor would be gone in its entirety. However people conducting criminal activity would be able to know if they are under the microscope. A free internet would thus not be controllable in the same sense as the current one, which could lead to a decrease in societal security. But how big of an impact does the NSA surveillance really have? Reports state that the NSA programs are much less effective in preventing terrorist attacks than traditional methods, and were only reponsible for a very small fraction of the cases[11, 12]. With this in mind you could argue that we are sacrificing some of our freedom and

privacy by living in an increasingly *big brother-esque* society for very little gain.

5.2 Censorship

In terms of censorship, decentralisation would mean that no one can easily remove data and thus censorship would be difficult. Also due to complete transparency, you would know if a government had been censoring content, making the censorship less effective. However do we want certain content censored? Some content are against the law and should by law not be easily accessible like anything else that is forbidden. Shutting down such sites are not censorship. It is not different than that of a physical shop being shut down due to violation of the law, so I would not coin this as "censorship". It is ethical correct to remove child pornography from the internet – the issue is the methods. An invisible DNS blocking, that can easily be extended to other sites without users knowing. There is a reason for why this is the method though, and this is where the borderless global society of the internet clash with national laws. It is very difficult to just erase content since it can be stored on a server anywhere in the world where the laws are different. It is simply not possible to actually shut down the services in some cases. However, due to the invisibility factor of computer technology it is much easier to secretly censor content. Decentralisation would too solve this issue, it would however also be harder to shut down illegal content.

6 Conclusion

In this paper I have investigated how a technology like Ethereum would decentralise computing and the ramifications that would have on society. I have outlined the current landscape of central governing units and corporations and dealt with ethical questions in these topics by using the theories defined by Wiener and Moor while commenting on these with Greenwald thoughts on surveillance in society. To sum up, in today's world a lot of unethical operations are happening due to intransparency. Our data from social networks

are free to use for corporations and are tapped by government surveillance programs. Our privacy is compromised, and thus our freedom as human beings. Decentralisation would mean giving up some governing control which in the end could lead to a decrease in security. It would though also offer a more free and transparent society. A society that according to Wiener would support human flourishing.

References

[1] Vitalik Buterin. *White Paper: A Next-Generation Smart Contract and Decentralized Application Platform*. 2013. URL: https://github.com/ethereum/wiki/wiki/White-Paper (visited on 05/09/2015).

[2] T. Bynum. *"Computer and Information Ethics", The Stanford Encyclopedia of Philosophy*. 2008. URL: http://plato.stanford.edu/archives/spr2011/entries/ethics-computer/ (visited on 05/09/2015).

[3] James Cook. *FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0*. Nov. 4, 2014. URL: http://uk.businessinsider.com/fbi-silk-road-seized-arrests-2014-11?r=US (visited on 05/09/2015).

[4] David Francis. *5 Reasons Why The NSA's Massive Surveillance Program Is No Big Deal (And 2 Reasons It Is)*. June 11, 2013. URL: http://www.businessinsider.com/nsa-surveillance-prism-phone-nsa-big-deal-2013-6?IR=T (visited on 05/09/2015).

[5] Glen Greenwald. *No Place to Hide: Chapter 4 - The Harm Of Surveillance*. 2014.

[6] Glen Greenwald and Ewen McAskill. *NSA Prism program taps in to user data of Apple, Google and others*. June 7, 2013. URL: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (visited on 05/07/2015).

[7] Anne Helmond. *The new Facebook data policy: like or dislike?* Feb. 12, 2014. URL: http://policyreview.info/articles/news/new-facebook-data-policy-or-dislike/341 (visited on 05/07/2015).

[8] Laura Hood. *Google's terms and conditions are less readable than Beowulf*. Oct. 17, 2013. URL: http://theconversation.com/googles-terms-and-conditions-are-less-readable-than-beowulf-19215 (visited on 05/07/2015).

[9] Victor Luckerson. *7 Controversial Ways Facebook Has Used Your Data*. Feb. 4, 2014. URL: http://time.com/4695/7-controversial-ways-facebook-has-used-your-data/ (visited on 05/10/2015).

[10] James H. Moor. *What is computer ethics?* 1985. URL: http://www.ccsr.cse.dmu.ac.uk/staff/Srog/teaching/moor.htm (visited on 05/07/2015).

[11] Ellen Nakashima. *NSA phone record collection does little to prevent terrorist attacks, group says*. Jan. 12, 2014. URL: http://www.washingtonpost.com/world/national-security/nsa-phone-record-collection-does-little-to-prevent-terrorist-attacks-group-says/2014/01/12/8aa860aa-77dd-11e3-8963-b4b654bcc9b2_story.html (visited on 05/10/2015).

[12] Meghan Neal. *You'll Never Guess How Many Terrorist Plots the NSA's Domestic Spy Program Has Foiled*. Jan. 13, 2014. URL: http://motherboard.vice.com/blog/youll-never-guess-how-many-terrorist-plots-the-nsas-domestic-spy-program-has-foiled (visited on 05/10/2015).

[13] *Nobody reads terms and conditions: it's official*. Apr. 19, 2010. URL: http://www.out-law.com/en/articles/2010/april/nobody-reads-terms-and-conditions-its-official/ (visited on 05/07/2015).

[14] Karim Pedersen. *Danske internet-udbydere kritiseres for censur*. Jan. 26, 2006. URL: http://www.computerworld.dk/art/153259/danske-internet-udbydere-kritiseres-for-censur (visited on 05/10/2015).

[15] Oliver Smith. *Facebook terms and conditions: why you don't own your online life*. Jan. 4, 2013. URL: http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html (visited on 05/07/2015).