# UNIVERZITA KARLOVA

FAKULTA SOCIÁLNÍCH VĚD

Institut sociologických studií


# Diplomová práce


**2017** **Bc. Martin Tremčinský**

# UNIVERZITA KARLOVA

FAKULTA SOCIÁLNÍCH VĚD

Institut sociologických studií

**Bc. Martin Tremčinský**


# Identity plug-ins: Towards post-human theory of informational privacy

*Diplomová práce*


Praha 2017

Autor práce: **Bc. Martin Tremčinský**
Vedoucí práce: **Mgr. Jakub Grygar Ph.D.**

Rok obhajoby: **2017**

**Bibliografický záznam**

TREMČINSKÝ, Martin. *Identity plug-ins: Towards post-human theory of informational privacy*. Praha, 2017, 47 s. Diplomová práce (Mgr.). Univerzita Karlova, Fakulta sociálních situdií, Insitut sociologických studií. Vedoucí práce Mgr. Jakub Grygar Ph.D.

# Abstrakt

Tento text se zabývá informačním soukromím v infosféře. Infosféra podle Luciana Floridiho představuje nový druh techno-vědecké ekologie, ve které se západní společnosti organizují a fungují. Soukromí je formulováno jako dělící práce v infosféře, kde každý (quasi)subjekt mobilizuje různé aktéry, aby uchránil své vnější hranice a odporoval objektivizaci. Dělící práce v infosféře je potom porovnána s podobnými typy aktivit v odlišných ekologiích a společnostech (např. Amazonský prales a Mongolsko)v zájmu identifikace klíčových aktérů, vykonávajících tuto dělící práci, založenou na zjednávání kategorií jako lidský/mimo-lidský, vlastní/nevlastní. Text rozlišuje tři typy dělících aktérů vycházejících ze tří vzájemně propojených narušitelů soukromí: obchodníků, dohlížitelů a zločinců. Argument je poté takový, že mobilizací různých dělících aktérů, závislých na typu narušitele, vznikají různé (quasi)subjekty, takže subjektivita je politický projekt spoluutvářený mimo-lidskými dělícími aktéry. Poslední část práce pak nabízí obecná etická východiska, která by mohla být v budoucnu užitečná, při řešení problémů spojených s informačním soukromím.

# Abstract

The text is concerned with informational privacy in infosphere. Infosphere according to Luciano Floridi presents a new type of techno-scientific ecology in which western societies organize themselves and operate. Privacy is conceptualized as a labor of division in the infosphere, where every (quasi)subject is mobilizing various actors in order to protect her outer boundaries and resist objectification. The labor of division in infosphere is then compared with similar types of labor in different ecologies and societies (i.e. Amazonia and Mongolia) in sake of identification of crucial agents carrying out this labor of division based on negotiations of categories such as human/non-human or self/non-self. The text distinguishes three types of actors of division according to three interconnected intruders; traders, overseers and criminals. The argument then is that through mobilization of various dividing actors depending on the type of intruder, different (quasi)subjects

emerge, thus subjectivity in the infosphere is a political project co-constructed by non/human dividing actors. The last chapter than proposes general ethical directions which might be helpful in the future, when considering the problems of lack of privacy.

## Klíčová slova

Post-humanismus, soukromí, Cyborg anthropology, ontologická politika, mnohočetnost, infosféra

## Keywords

Post-humanism, Privacy, Cyborg anthropology, ontological politics, multiplicity, infosphere

**Rozsah práce:** 149 885 znaků

### Prohlášení

1. Prohlašuji, že jsem předkládanou práci zpracoval/a samostatně a použil/a jen uvedené prameny a literaturu.
2. Prohlašuji, že práce nebyla využita k získání jiného titulu.
3. Souhlasím s tím, aby práce byla zpřístupněna pro studijní a výzkumné účely.

V Praze dne … Bc. Martin Tremčinský

## Acknowledgments

Here I would like to thank to my supervisor dr. Jakub Grygar and consultant doc. Martin Hájek for their comments and support. I also want to thank my parents and family for their support in moments of despair and for their patience with my mood swings. My endless gratitude goes all the way back to Enschede, to “Twente Boys” for incredibly stimulating environment they provided me with during winter semester 2016, without you guys I wouldn’t be the cyborg I am now. Namely I would like to thank to “warrior queen” Alice Fox, The Finn, and also to my Czech “sorcerer” Jan Tesárek, you all helped me more than a lot and I owe you big time! Last but not Least I would like to thank to John Doe for being my guide in the realm of information in which I would otherwise get lost forever.

# Institut sociologických studií
# Teze diplomové práce

**Projekt diplomové práce**

Světovými médii nedávno proběhla série zpráv informující o sporu FBI a americké společnosti Apple, jenž opět upozornil na problémy spojené se současnými technologiemi. V diskuzi opozičních táborů se projevil konflikt mezi dvěma důležitými kulturními hodnotami, právo na soukromí a fyzické bezpečí jedinců. Mobilní telefon iPhone zabitého teroristy Syeda Farooka, se tak stal jedním z aktérů v kontroverzi dvou (zdánlivě) vzájemně se vylučujících postojů, které jedinci i instituce zaujímají k úloze státní moci v západní společnosti. Zatímco FBI se snažila získat informace o mrtvém teroristovi, společnost Apple se bránila, že vytvořením zadních vrátek, která by tento průnik umožnila, ohrozí soukromí všech svých zákazníků.

To, co mě na kauze zaujalo, a proč na ni upozorňuji, je přítomnost specifického mobilního telefonu, konkrétního materiálního předmětu, který se v ní stal klíčovým aktérem. Můžeme tak hovořit, podobně jako Jane Bennett (2010, 108), o politice materiálních předmětů umožňujících lidské jednání. Farookův telefon se totiž stal svědkem, aktérem ve vyšetřování, který měl poskytnout klíčové informace vzhledem k tomu, že terorista byl již v době vyšetřování po smrti. To ukazuje, že technologie jsou více než jen našimi prodlouženími, jsou formou určitých společenských inskripcí. Komunikační technologie nás tak například svými atributy vyzývají k vytváření, ukládání a sdílení široké škály osobních dat. Zároveň je možné vnímat technologii jako materiální vyjádření společenských mocenských struktur, které umožňuje držet společnost pohromadě v konkrétní podobě jako „odolný celek“. (Latour 1990, 103) „Technologie a společnost netvoří dvě ontologicky oddělené entity, ale spíše dvě fáze stejné esenciální aktivity.“ (ibid. 129)

Dichotomii soukromý/veřejný se věnuje řada sociologů (např. Simmel 1950, Goffman 1963, Hall 1966, Schwartz 1968, Altman 1977), díky čemuž má soukromí mnoho definic. Simmel (1950, 330-331) nehovoří přímo o soukromí, ale používá termín tajemství (*secrecy*), které definuje jako skrývání určitých realit pozitivními či negativními prostředky. Tajemství nabízí paralelní svět ke světu zjevenému (*manifest*) a jeho existence mezi/před jedinci či skupinami, pak podle Simmela výrazně ovlivňuje jejich vzájemné interakce. Goffman (1963, 157) pak vnímá soukromý především jako prostor, ve kterém se jednotlivci či skupiny připravují na své veřejné vystupování. Hall (1966, 104) navazujíce na Goffmana, vnímá soukromí dost obdobně, jako osobní prostor, nad kterým má jednotlivec kontrolu a může moderovat, kdo do něho vstoupí a kdo nikoliv. Zároveň tvrdí, že soukromí v západní společnosti vzniklo až v průběhu 18. století, kdy se začali oddělovat jednotlivé místnosti domů podle svých funkcí. Schwartz (1968, 741) definuje soukromí jako institucionalizované odstoupení (*institutionalized withdrawal*) ze sociální interakce. Zároveň uvádí, že soukromí a schopnost si ho udržet, respektive narušit soukromí jiných je vždy určitým vyjádřením moci. Altman (1977, 67) jej pak definuje jako selektivní kontrolu přístupu k self, jako proces vyjednávání hranic v interakci s ostatními.

Ovšem Simmel, Hall, Goffman, Schwartz i Altman ignorují vliv technologií na soukromí. Narušení se pro ně odehrává vždy jen v přítomném čase a v přímé interakci. Nejsložitější technologie, jakou jsou tito muži se soukromím a jeho udržováním/narušováním (vzhledem k době, ve které psali) ochotni spojit, jsou dveře, a to i přestože Hall upozorňuje na technologie jako na evoluční urychlení člověka (1966, 3). Mnohem pohotovější se v tomto ohledu ukázali teoretici práva Warren a Brandeis, kteří upozorňují na strach spojený s rozmachem nových technologií (konkrétně novin a fotografie) a

jejich dopadem na soukromí už v roce 1890 ve svém článku *The Right to Privacy*. Z jejich článku vyplívá, že už v 19. století se lidé obávali, že díky technologiím nebudou schopni mít kontrolu and vlastním obrazem, že se stanou *objektem* v rukou jiných.

Nejjednodušší definicí soukromí zohledňující i vliv technologií a díky tomu nejvhodnější pro můj výzkum se mi tak jeví ta od filosofa Rolanda Barthese z jeho knihy o fotografii *Světlá komora*: „'Soukromý život' není nic jiného než ona výseč prostoru a času, v níž nejsem obrazem, objektem. *Je mým politickým právem být subjektem*, které musím bránit." (2005, 21, kurzíva přidána) To co je na této definici tak elegantní a podle mě i přínosné je, že operuje s minimem sociálních institucí jako je skupina, domov, společnost. Vystačí si v podstatě s jednoduchou dichotomií subjekt/objekt, která je (za pomoci technologií) ostatními napadána.

Ve své práci bych se chtěl zaměřit právě na vyjednávání soukromí skrze technologie. Na utváření a rozpoznávání hranic mezi self a other, jež se díky technologiím mění. Podle Donny Haraway je „individualita problémem strategické obrany. Člověk by měl očekávat, že kontrolní strategie se budou zaměřovat na údržbu hranic a rozhraní (interfaces), na stupně toků skrze hranice a ne na integritu přírodních objektů." (1991, 212) Dále Haraway tvrdí, že tak mizí ontologická hranice mezi organismem a technologií (ibid.), z čehož plyne, že pokud chceme studovat současné soukromí, musíme se, místo na lidskou rezistenci vůči technologickému sledování, zaměřovat na lidsko-technologickou rezistenci vůči lidsko-technologickému sledování.

Zároveň pokud připustíme, že soukromí a jeho narušování ostatními má klíčový vliv na formování našeho self, pak naše self se proměňuje v závislosti na našich (nejen) technologických možnostech si soukromí uchránit. Stáváme se tak kyborgy a to nejen ve smyslu využívání technologických prodloužení našich těl, ale především ve změně perspektivy vnímání a reflexe nás samotných (Lupton 2012).

Data, která o sobě shromažďujeme a ukládáme do různých technologických zařízení, jsou našimi doprovodnými druhy (companion species), jež mají vlastní život částečně mimo naši kontrolu (Lupton 2016, 3). Tyto companion species ovšem neexistují nezávisle na nás, jsou s námi vnitřně spjaty a utvářejí naše kyborganická self. „Být jedním vždy znamená stávat se s mnohými." (Haraway 2008, 4) Kauza FBI vs. Apple může sloužit jako jeden z mnoha příkladů sporů o to, kdo bude s těmito companion species v kontaktu a bude se podílet na jejich kontrole.

Prostřednictvím polostrukturovaných rozhovorů, etnografických pozorování a analýzou dokumentů plánuji zjišťovat, jak jsou jednotliví lidští a mimolidští aktéři vzájemně propojováni a jak se toto propojení odráží v naší reflexi okolního světa. Pokusím se zevrubně popsat za pomoci jakých aktantů je naše soukromí performováno, v jakých situacích se vyjevuje a jaká self utváří. Zároveň se budu snažit udržet si pokud možno co nejvíce pohled zvenčí. Díky tomu, že kromě notebooku nevyužívám smartphone, tablet, podkožní implantát či jiná mobilní komunikační zařízení, mohu si od zkoumaného terénu udržet jistý odstup, přistupovat k němu jako k něčemu novému a neznámému (Latour 2007, 80-81). Sledování jednotlivých praktik spojených s technologií by tak pro mě mělo být vždy závislé na porozumění a interpretaci samotných aktérů. Budu sledovat jaká rizika s informačními technologiemi spojují a jak se jim snaží vyhnout; jaké používají prohlížeče a aplikace, k čemu všemu používají informační technologie (komunikace, platby, odemykání dveří) a jaké další anonymizační techniky využívají (masky, modulace hlasu, nálepky přes kamery). V neposlední řadě se zaměřím na metafory, jež jim pomáhají komunikovat problematiku křehkosti soukromí s okolním světem (například umělecké instalace, fotografie, či provokace).

Za účelem rozhovorů plánuji oslovit jednotlivce, kteří se pohybují v oboru IT security jak profesně, tak i jako aktivisté. Tuto úzce vymezenou skupinu komunikačních partnerů jsem si zvolil, protože

věřím, že mi nejen pomohou efektivně rozkrýt síť aktantů podílejících se na produkci soukromí, ale také protože je vnímám jako jedny z důležitých aktérů v tomto procesu. Jejich význam pro soukromí spočívá v tom, že upozorňují na jeho narušení, čímž podle mě zásadně přispívají k formování jeho hranic. Etnografické pozorování pak chci provádět na jejich veřejných setkáních pořádaných například organizací Paralelní polis, na festivalu Kryptofest, nebo na konferenci Cyber Security and Internet Safety. Takto získaná data bych pak chtěl propojit i s analýzou textů publikovaných jak na specificky zaměřených webech (např. s3c.cz) tak i na běžných zpravodajských portálech (např. novinky.cz).

K analýze dat plánuji využít přístup tzv. „cyborg anthropology" (Downey, Dumit, Williams 1995), který umožňuje kombinovat přístupy ANT, STS, post-fenomenologie a další. Tento přístup zkoumá současnou vědu a technologii jako kulturní aktivity, přičemž se zaměřuje na to, jak je naše lidskost produkována skrze stroje. Snaží se tím najít alternativy k tradičnímu karteziánskému rozdělení subjekt/objekt, tím, že zkoumá a rozvíjí post-strukturalistický a post-humanistický argument, že „lidské subjekty a jejich subjektivita jsou stejně tak zásadní funkcí strojů, vztahů se stroji a informačních přenosů, jako jsou operátory a producenty těchto strojů." (Downey, Dumit, Williams 1995, 266) Nejvíce bych při tom chtěl vycházet z prací Johna Law (2004) a Annemarie Mol (1999), podle kterých jsou multiplicitní ontologické reality performovány uspořádáním aktérů zvoleným k jejich ztvárnění (enactment) (Law 2004, 56; Mol 1999, 75).

Mé výzkumné otázky jsou pak vcelku jednoduché: jakým způsobem současné informační technologie spoluutvářejí (performují) soukromí? Jak se současné technologie stávají důležitým prvkem lidské sebereflexe?

Jejich zodpovězení by mělo přispět k pochopení dynamiky utváření technovědeckých ontologií. Chtěl bych tak přispět do diskuze o povaze našeho vlastního Self, které není ustavováno pouze v interakci s ostatními jedinci, ale i s mimo-lidskými aktéry. Zároveň bych svou prací také chtěl rozvíjet otázky, jež si kladou Hannah Knox a Antonia Warford (2016) v jimi editované sérii Digital Ontology zveřejněné na stránkách časopisu Cultural Anthropology. Otázkou totiž je nejen, jaké různé ontologie díky digitálním informačním technologiím vznikají, ale i zda vůbec nějaké digitální ontologie existují.

**Použitá literatura:**


Altman, I. (1977). Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues* 33 (3) 1977

Barthes, R. (2005). Světlá komora: poznámka k fotografii. Praha: Agite.

Bennett, J. (c2010). *Vibrant matter: a political ecology of things*. Durham: Duke University Press.

Downey, G. L., Dumit, J., & Williams, S. (1995). Cyborg anthropology. *Cultural Anthropology*, *10*(2), 264-269.

Goffman, E. (1963). *Behavior in public places: Notes on the social organization of gatherings* (p. 248). New York: Free Press.

Goffman, E. (1956). *Presentation of Self in Everyday Life*. Monograph No. 2. Edinburgh: University of Edinburgh. Social Sciences Research Centre.

Hall, E. T. (1966). *The hidden dimension: an anthropologist examines man's use of space in public and in private*. New York: Anchor Books.

Haraway, D. J. (1991). *Simians, Cyborgs, and Women: the Reinvention of Nature*. New York: Routledge.

Haraway, D. J. (2008). *When species meet* (Vol. 224). U of Minnesota Press.

Knox, H. and Walford, A. (2016) "Digital Ontology." *Theorizing the Contemporary,* Cultural Anthropology website, March 24, 2016. https://culanth.org/fieldsights/820-digital-ontology

Kohn, E. (2007) How dogs dream: Amazonian natures and the politics of transspecies engagement. *American ethnologist*, 2007, 34.1: 3-24.

Latour, B. (1990). Technology is society made durable. *The Sociological Review*, *38*(S1), 103-131.

Latour, B. (2007). *Reassembling the social*. Hampshire: Oxford University Press, 2007.
Law, J. (2004). *After method: Mess in social science research*. Routledge.
Lupton, D. (2012) M-health and health promotion: The digital cyborg and surveillance society. *Social Theory & Health*, 2012, 10.3: 229-244.
Lupton, D. (2016). Digital companion species and eating data: Implications for theorising digital data–human assemblages. *Big Data & Society*, *3*(1), 2053951715619947.
Mol, A. (1999). Ontological politics. A word and some questions. *The Sociological Review*, *47*(S1), 74-89.
Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology*, 741-752.
Simmel G. (1950) 'Secret and secret society' in Simmel, G., & Wolff, K. H. (1950). *The sociology of Georg Simmel* (Vol. 92892). Simon and Schuster.
Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.

**Orientační přehled další literatury:**

DOWNEY, Gary Lee a Joseph DUMIT. *Cyborgs & citadels: anthropological interventions in emerging sciences and technologies*. 1st ed. Santa Fe, N.M.: School of American Research Press, c1997. School of American Research advanced seminar series. ISBN 0-93345-296-9.
GELL, Alfred. *Art and agency: an anthropological theory*. 1st published. Oxford: Clarendon Press, 1998. ISBN 0-19-828014-9.
GRAY, Chris Hables a Steven MENTOR. *The cyborg handbook*. New York: Routledge, 1995. ISBN 978-0-415-90849-8.
HELMREICH, Stefan. *Silicon Second Nature: Culturing Artificial Life in a Digital World, Updated With a New Preface*. Univ of California Press, 1998.
LATOUR, Bruno. Reassembling the social. *Hampshire: Oxford University Press*, 2007.
LAW, John. Sociology of monsters? Power, technology and the modern world. *The Sociological Review Monograph*, 1991, 38.
LAW, John. *After method: Mess in social science research*. Routledge, 2004.
MURI, Allison. *The Enlightenment cyborg: a history of communications and control in the human machine, 1660-1830*. University of Toronto Press, 2007.
NISSENBAUM, Helen. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press, 2009.
STRATHERN, Marilyn. *Partial connections*. Updated ed. Walnut Creek: Altamira Press, 2004. ISBN 0-7591-0759-9.
VERBEEK, Peter-Paul. *What things do: Philosophical reflections on technology, agency, and design*. Penn State Press, 2010.

# Contents

# Identity plug-ins: Towards post-human theory of informational privacy

*Halber Mensch*
*Du siehst die Sender nicht*
*und Kabel hängen*
*längst verlegt*
*aus deinen Nerven*[1]
(Einstürzende Neubauten – Halber Mensch, 1986)

## 1. Introduction

I'm looking on a Polaroid picture of someone's bedroom. Two unmade beds are standing next to each other, side to side, in the far right corner of the room, right under the window. The blankets and pillows are crumpled in the same state as somebody left them in the morning, while leaving for work or maybe for school. There's a teddy-bear lying under one of the pillows. Everything seems normal. I don't know that bedroom, I've never been there, yet I'm getting goosebumps when I imagine what happened there.

The Polaroid picture is a part of German photographer Simon Menner's presentation, *What does Big Brother see, while he is watching?*[2] It used to be a part of secret Stasi archives. While showing this picture, Menner describes that Stasi – the former German Democratic Republic's secret police – used Polaroid to photograph rooms which they broke into for illegal raids, so they would be able to restore the rooms back to original state and nobody would notice that her privacy was invaded.

Even though this Polaroid photography now acts as a memento of recent unfortunate history, it used to be actual spying tool, an agent (see Verdery 2014). Most striking, is not the picture itself, but the situation it revealed and helped to create. Stasi's Polaroid depicts someone's bedroom, where the secret police operated without the owner's knowledge or consent. The Polaroid itself, a particular technological device, altered not only the working routine of Stasi spies; it also changed the world of those who were spied on, of their victims.

While watching Menner's talk, I remembered reaction of my mother few years back when her office was burgled. Her biggest concern was not about the stolen things, but about the *contamination* of space and things that were left in the office. I remember her throwing away everything from the fridge and kitchen. Opened crate of milk, can of coffee, pack of cookies, everything had to go, because she felt that it was polluted by the presence of the burglars. Even though they most probably didn't even enter the kitchen, because all electronic appliances stayed intact, just the idea that they drank her milk, or touched her food prohibited her from keeping these stuff. But unlike the victims of Stasi, my mother knew that her

[1] Translation: "Half man, you don't see the transmitters and cables, laid long ago hanging from your nerve." (neubauten.org)
[2] Talk given 1.10.2016 during Hackers Congress Paralelní Polis (HCPP2016). Described photo can be found on Meners web page: http://simonmenner.com/pages/Stasi-Polaroid1.htm

personal space had been compromised immediately, whereas Stasi's targets rarely were graced with that knowledge until many years later, if at all.

Unfortunately, in the 21st century it is not a Polaroid, with its abilities of visual conservation, which threatens our privacy. Rather, one of the most discussed technologies changing our privacy in current days seems to be the internet and the information and communication technologies (ICTs). Indeed on Czech most read news service website *Novinky.cz*, there's a new message, concerned with internet privacy and security, published almost every day (and it is not only Czech phenomenon, the same can be said for example about Britain's *Guardian*).

Moreover, on the internet we also, like the Stasi victims, cannot know whether our personal space or data are being contaminated and if so, by whom. Boundaries of our personal (cyber)space become uncertain; every once in a while a newsflash occurs informing us about another leak of passwords, NSA spying on half of the Europe, or a new software exploit enabling the intruders to spy on us via our smart TVs. All these events are like the opening of Stasi archives, they *post-factum* show the extent of contaminated space.

This work is rooted in the post-structuralist critique of western dualism dividing the world on subjects and objects. The critique is not based on denying such division but rather on questioning it and criticizing the ontology in which this division is naturalized and treated as *matter of fact*. The destabilization of this dominant western ontology allows me to think *otherwise.* By revealing the different worlds this ontology often renders invisible, it becomes more clear why privacy is a politically motivated activity depending on cooperation of various actors.

If we define privacy by a simple definition that "privacy is a political right to remain subject" (Barthes 1981, 15) privacy is not seen as a struggle to maintain and protect *social identity,* but rather seen as an *ontological identity* – given that subject and object are not social but ontological categories.

In order to apply such simple definition, it is necessary to clarify what is meant by subject and object in reality: denouncing these categories as *matters of fact* and reconstructing them as *matter of concern.*

Since, according to Schwartz, privacy is considered one of the key stones of self-definition (1968, 747). Every new technology enabling its protection or invasion acts as a potential *individualizer*, co-producer of our individual selves or, as Bruno Latour called it: a *plug-in* (2007, 207).

According to American Bitcoin evangelist Andreas Antonopoulos, "privacy is costing, it takes effort" and it "is not easy."[3] By these words, Antonopoulos implies that internet privacy is neither in our possession, nor is it a *state of affairs*; on the contrary, it is an activity--something which has to be *enacted* repeatedly through various actors in order to be successful. We can even find an analogy for this in our material environment, namely in the activity of locking our doors. We don't have to lock our doors just once and then we are safe; we have to lock them every time we leave the house, if we want to keep unwanted intruders out of our private space. Similarly, if we want to have control over our privacy on the internet:

[3] Andreas Antonopoulos' talk named *Thoughts on the Future of Money* which took place on 1.10.2016 at HCPP2016.

we have to update our antivirus software; we have to avoid opening suspicious messages; we have to protect our passwords, etc.

What is more, we have to deploy different strategies and different activities to protect ourselves from different intruders; and because we cannot protect ourselves from an intruder, of which we do not have at least a blurry image, we can say that potential intruders and their modes of violation are crucial to the enactment of privacy. As intruders vary from pirates and malware, to corporations and service providers, to governments and secret services, knowledge of various defense strategies are required.

Hence, as in different methods of diagnosis in Annemarie Mol's theory enact multiple phenomena (1999, 85), I claim that different methods of possible *privacy invasion* enact multiple privacy. The questions surrounding this topic are: Which intruders, technologies or *plug-ins* help us to enact multiple kinds of internet privacy? How do they enact such kinds of privacy? And thus how do they participate in our self-making? By answering these questions, I hope to provide clarity and depth to broader field of *cyborg anthropology*.

I use in this text a variety of concepts from sociology, anthropology and philosophy in order to offer an analytical perspective which may be well suited for investigating diverse socio-technical phenomena. My goal is not to provide one straight answer to problems of privacy on the internet; I try to suggest new ways how to re-conceptualize what it means to live in informational ecology instead. My work is thus mainly theoretical using deductive method of reasoning, rather than empirical and inductive; although I use some empirical experiences to illustrate my theoretical conclusions. The aim is thus to provide a description of informational privacy while avoiding modernist assumptions of intangible subject/object divide, which would allow new forms of political action.

In the last chapter I then offer some ethical consideration. By using Kant's deontology I argue that the enactment of reality is an ethical problem which includes multiple actors. I propose that in order to avoid certain asymmetries we have to avoid the modern tropes of elimination by domination and focus more on mutual co-existence of various modes of being embodied in alternative assemblages.

## 2. Social theory of privacy

The increasing prioritization of privacy is deeply interlinked with modernity. Jean Jacques Rousseau described the inventor of private property as the "founder of civil society" with all its sufferings, problems and negatives (Rousseau 2002 [1762], 113-14).[4] Of course his analysis is hardly to be considered historical; we can speak rather of an *origin story* (Roberts 2016). Nonetheless Karl Marx and Max Weber also connected private property with the opportunities to accumulate capital and give rise to the modern age (Marx & Engels 2002 [1888], 48; Weber 2001 [1930], 107).

[4] "The first man, who after enclosing a piece of ground, took it into his head to say, *this is mine*, and found people simple enough to believe him, was the real founder of civil society. How many crimes, how many wars, how many murders, how many misfortunes and horrors, would that man have saved the human species, who pulling up the stakes or filling up the ditches should have cried to his fellows: Beware of listening to this impostor; you are lost, if you forget that the fruits of the earth belong equally to us all, and the earth itself to nobody!" (Rousseau 2002 [1762], 113-14)

But this text is not concerned with the importance of private property and its impact on contemporary subjectivity, as this was thoroughly covered by the aforementioned giants of social science. My text is concerned with the informational privacy, therefore not the right to control tangible goods as personal belongings, but the right to control individual information as part of the self (Floridi 2014, 120).

## a. Right to privacy

One of my colleagues recently told me that privacy is the new defining concern of our time. That what was a hundred years ago discussed in terms of liberties, nowadays is discussed in terms of discretion. However flattering to me and my topic it felt at the moment, I have to admit that such reasoning would be a mistake. The worry about informational privacy and how it's affected by new technologies is not that new in modern society. Already in 1890 Samuel D. Warren and Louis D. Brandeis published their today almost canonical article *The Right to Privacy* where they urgently called for new legislative tools securing the "right to enjoy life and to be let alone" (Warren and Brandeis 1890, 193). It is striking how similar to current situation were the worries concerning privacy and technology more than 125 years ago:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone. " Instantaneous photographs and news- paper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." (Warren and Brandeis 1890, 195)

Warren and Brandeis focus mostly on the individual's right to protect her good name; therefore gossip and its spread is in their view the main breach of privacy against which people shall be institutionally protected. Given the nature of the technology and its modes of use, their main concern is to protect the wealthy people form the peeping eye of the press, mediating the life of the upper class to the publics to satisfy the latter's *prurient taste* (1890, 196).

The raise of new information technologies as photography and printed newspapers then change the nature of gossip from vicious joy of the idle to an object of trade (1890, 196). Personal privacy in their account therefore becomes an informational currency. Similarly as today the breach of privacy is what is *paid with* and maintaining privacy is what is *paid for* (Schwartz 1968, 743). The emergence of the informational society is connected with the appearance of new economy where personal information about self and others become highly valuable assets. This commodification of privacy is in Warren's and Brandeis' eyes harmful to the wellbeing of an individual, inflicting pain comparable to or rather exceeding harm inflicted upon her body (1890, 196). In other words attack on privacy is act of violence against the modern subject.

The informational privacy and emergence of modern subjectivity are historically intertwined entities mutually constructing each other. Barry Schwartz argues that the modern privacy emerges with the appearance of the middle class and its wide application of inner doors in households and differentiation of the particular rooms with limited access by individual members. Placing a barrier between self and others is in fact a *self-defining* practice

(Schwartz 1968, 746-48). Violation of this boundary is a violation of selfhood, because the subject can no more control her audience and regulate access to her individuality. Schwartz further provides an example of *total institutions* such as prisons, or the army where the lack of privacy serves a simple purpose to mortify the self and make eventually absent the whole consciousness of self (1968, 749; see also Goffman 1961).

In conclusion it may be said that Schwartz defines privacy as "highly institutionalized mode of *withdrawal*" (Schwartz 1968, 741). Privacy is according to him social phenomena, which is necessary for right functioning of social groups, because it poses a structure of social order. This structure then regulates who have access to others and the right to manipulate them. Unfortunately the only truly historical grounding of modern privacy in Schwartz's work is based on the relatively new experience of personalized space within the household. More contemporary approach may show what other experiences provided by modern institutions helped to construct modern privacy.

## b. Privacy according to Anthony Giddens

One of the contemporary sociologists dealing with modernity, privacy and its influence on formation of self is Anthony Giddens. In *The Consequences of Modernity* (1990) and *Modernity and Self-identity* (1991) Giddens describes the changes in modern life and self-identity through rapid changes in institutional setting in which are our own selves situated. According to Giddens "[m]odernity must be understood on institutional level; yet the transmutations introduced by modern institutions interlace in a direct way with individual life and therefore the self." (1991, 1)

For Giddens the formation of modern self-identity is a reflexive project based on considerations of risks and dangers filtered through contact with expert systems. (1991, 5) But these expert systems are in Giddens' account merged together with symbolic tokens into *abstract systems* (1990, 80) which then filter our reflexive project of the self (1991, 5). "[A]bstract systems become centrally involved not only in the institutional order of modernity but also in the formation and continuity of the self." (1991, 33) Abstract systems thus present for Giddens deterministic boundaries in which self is allowed to develop and operate.

Privacy is then defined by Giddens in two ways, which are both associated with the development of modernity (1991, 151). In its first sense, privacy is shaped by the institutions of the *state* and *civil society*, where civil society stands opposed to the penetration of the state into everyday life, in the same way as the private opposes the public (Ibid.). Privacy is then described as a domain "which resists the encroachment of the state's surveillance activities," but on the other hand is also positively legally defined by the state as the guarantor of law (Ibid.).

The second sense suggests that the private/public opposition is concerned with concealment and revelation to others. Such opposition is established through the emergence of modern *society of strangers;* that is the moment when the traditional *stranger* ceased to exist and was replaced by the *civil indifference.* (1991, 151)

> The wide arenas of nonhostile interaction with anonymous others [or *civil indifference*] characteristic of modern social activity did not exist [in traditional society]. In these circumstances, friendship was often institutionalized and was seen as a means of

> creating more or less *durable alliances* with others against potentially hostile groups outside. (1990, 118, emphasis added)

The modern concept of privacy as concealment is then according to Giddens directly related to the institutional *invention of childhood*:

> Privacy, and the psychological needs associated with it, were almost certainly strongly conditioned by a further separation, that of childhood from adulthood. […] The emergence of a separate province of `childhood' demarcated the experience of growing up from outside arenas of activity. Childhood became concealed and domesticated, as well as subject to the core influence of formal schooling. As childhood is separated out from the activities of adults, or at least shaped in distinctive ways, it forms an area of concealment within which private experiences are structured. (1991, 152)

In this historical account institutionalized childhood as a private experience becomes source of infrastructure for personality. (1991, 153)

To sum up, Giddens provides us with two interrelated historical accounts of privacy, which signify the rise of institutions of modernity and distinguish it from the traditional society. Our private subjectivity is then formed by our encounters with abstract systems of modern institutions, organized mainly by the state.

State provides us with legal definitions of privacy and state institutions are supposed to protect those boundaries. Everything that is outside those state set boundaries belongs to the public and is thus subjected to the state surveillance (but as we saw with the Stasi case, these boundaries can be violated by state power).

State also provides us, through schooling system and other institutional definitions of childhood, with the source of experience of privacy. This experience according to Giddens forms our personalities as modern people distinguishing between private and public.

### c. Critique of Giddens

This brings us to the matter of sufficiency of Giddens' account of privacy. Even though Giddens describes identity as self-reflexive project where "individuals help actively to reconstruct the social universe around them" (1991, 12), this self-reflection seems very tightly bound by the limits set by *abstract systems*. The problem is that (not only online) privacy is under thread of violation by different actors on daily basis and its boundaries are not established merely by social contract, on the contrary these boundaries have to be enforced by practices consisting of human and non-human actor assemblages. Although state serves as a protector of privacy, it is difficult to legally prove breach of informational privacy for there is nothing gone missing. That is because private information is not a belonging in terms of property; private information is belonging in terms of constituting the subject (Floridi 2005, 195). And at the same time the state's capacity for surveillance (and thus setting the boundaries of public/private divide) is co-shaped by technology.

Institutions, individuals and technologies have to work together in order to be successful. Giddens provide us with good analysis of how the institutions participate in self-making process. Unfortunately Giddens' account doesn't provide us with description of the agents and actants through which these institutions are able to do so. If we borrow a little critique from history of technology, we can say that Giddens is concerned with the *invention* of privacy but doesn't speak much about its *maintenance* (McCray 2016). In other words, his abstract

systems remain too abstract and his analysis does not inform us how and by whom (or what) is the establishment and security of privacy carried out. Isn't our struggle for privacy the same process of formation of durable alliances, which were by Giddens described as traditional friendship? Respectively aren't nowadays these alliances created only by different actors to protect our-selves from different types of *outsiders*?

This is because Giddens' notion of privacy is social. Giddens *black-boxes* human subjects as social actors and privacy represents basically exchange of information between these mutually exclusive actors. But if we accept Latour's proposition that the division on subject and object is actually artificial and introduce to our social reality also non-human actors as carriers of action it opens up new dimension for understanding of privacy.

Thanks to reduction of the whole reality to non-hierarchically spread actors (Latour 2007, 171-72) the comprehension of privacy becomes an ontological problem. If one is never a pure type but consist of many (Haraway 2008, 4), always being constructed through interaction with various actors, privacy becomes a boundary work through which one tries to control which actors are enabled to perform in her personal assemblage called *self*. This self can be defined as a quasi-subject, an experience of being in and being able to act upon the surrounding world (Rey & Boesel 2014, 176).

In this line of thought self is not a cultured only through institutions, but on the other hand self is an outcome of encounters with the ecology surrounding and co-shaping the individual body (Kohn 2013, 16). Thus to be able to grasp informational privacy (as a form of self-culturing) in contemporary western society, we have to ask about the ecology in which the self emerges.

Luciano Floridi (2014, vii) describes our current ecology as an infosphere. Infosphere emerges through interconnection of information which is unprecedented in scale of time and space. Unlike modern view on information technologies, in which these acted like extensions of human, the current information and communication technologies (ICTs) are described as co-shaping the whole time-space in which western societies operate (Floridi 2014, 97).

But it would be unfortunate to reduce current ICTs only to flow of information; that would lead to same degree of abstraction as Giddens' abstract systems. In order to better understand the ecology of the infosphere we shall focus on its design and its properties. In this task might come very helpful the concept of *hyperobject* introduce by Timothy Morton.

## 3. Ontology politics

In order to be able to analyze the ontological shaping of private identities, allow me first to introduce the general metaphysical dimensions in which my text operates and which I am trying to enact through my writing.

Realities and their enactment are closely related to the environment in which they take place. That is the basic claim of so called *ontological turn* in social sciences. According to Mario Blaser, this focus on ontology as something social is based on the crisis of western dualism (Blaser et.al. 2013, 556). Western society up till the twentieth century accepted its own reality as an objective reality *out there* which is independent on practices which describe it; as a reality of ahistorical facts, which wait to be discovered. This situation is nowadays known as Cartesian dualism; a historical moment which naturalized the distinction of subjects

and their perspectives on reality from inert objects, constituting building stone of such "objective" reality.

But recent works of philosophers of science, sociologist and social anthropologist show, that the emergence of *objective* reality is not independent from the actors which bring it into being (see i.e. Barad 2007; Latour 1993; Law 2004 etc.). These claims are further supported by anthropologists analysing other than western realities (i.e. De Castro 1998; Kohn 2013; Pedersen 2011; etc.). The fundamental claim is that other cultures with other views, practices and environments enact other realities; that their answer to the philosophical question about the nature of reality drastically differs and that there is no way to distinguish which reality should come prior to others (Blaser et. al. 2013, 550).[5] Thus we cannot speak of cultural relativism, because relativism still implies an objective reality *out-there* whereas the culturally determined perspective is just a domain of the subject. Such an approach is still rooted in Cartesian time-space; we can speak rather of realism, namely the speculative realism which implies multiple realities brought into being by interactions of multiple actors (Harman 2009, 72).

In the western world making the leading roles were carried out by science and technology. In traditional view *science* describes what the reality is made of and *technology* helps us to shape it. But in the view of some more radical thinkers this is not the case. Their argument is that subject and object – same as nature and culture – are outcomes of negotiations.

## a. Science as world making process

French sociologist and philosopher Bruno Latour argues that *science* actually creates and negotiates its object – usually known as Nature – in scientific controversies, and then retrospectively naturalizes it: "As long as controversies are rife, *Nature* is never used as the final arbiter since no one knows what she is and says. But once the controversy is settled, *Nature* is the ultimate referee." (Latour 1987, 97) And what's more Latour claims that this does not apply only to *Nature*, but also to *Society:*

> That society stands in the way of sociology and of politics is not so surprising for those of us in science studies who saw earlier how nature, too, stood in the way. Both monsters are born in the same season [of enlightment] and for the same reason: nature assembles non-humans apart from the humans; society collects humans apart from the nonhumans. […]After nature, it is society that has to go. If not, we will never be able to collect the collective. (Latour 2007, 164)

By collective Latour means association of humans and non-humans which together bring the reality into being. Thus for Latour society and social phenomena are not resources for action but outcome of action (2007, 64). For Latour actors emerge in their mutual interaction (Harman 2009, 65) and thus humans – previous domains of society – participate in making of nature and non-humans – previous domains of nature – participate in making of society.

[5] The questioning of hegemony of ontologies is not just mere theoretical problem, but according to Eduardo Kohn, has very serious impacts in real life. In Kohn's view if we let some ontologies win over the others, it means that some realities will inevitably disappear (Kohn 2013, 227).

Humans and non-humans are in Latour's view both equal actors in social interactions. That is the reason why Latour calls his approach symmetrical anthropology (1993). This symmetry is attack on the subject/object or culture/nature dualisms. In the view of Latour and other STS authors subject and object are not ahistorical facts. Quite the opposite both has to be made, enacted, performed. But they are not performed only by one set of actors, human or non-human (1993, 55); quite the opposite objects and subjects are performed by assemblages of humans and non-humans forming what Latour calls quasi-objects and quasi-subjects. The culture as realm of subjects and nature as realm of objects are simply not causes but outcomes of various negotiations between various actors. In words of Donna Haraway: "the one can no longer be the resource for appropriation or incorporation by the other." (Haraway 1991b, 155)

According to sociologists John Law and John Urry (2004), to write about society, is to engage in *ontological politics*. In their article *Enacting the social* Law and Urry describe how scientific practice (not only) in social sciences does not produce a mere description of social worlds, but it helps to create social realities (2004, 390-91). In other words social science is *performative* (2004, 395).

Nevertheless saying that social reality is performed or constructed does not mean that this reality is not real; "it is both *real* and *produced*". (Law and Urry 2004, 396, emphasis added) One of the most notorious examples of this performativity of social science can be found in Marxism. Marx's reality enactment of class struggle has been incredibly successful in shaping what we call the global history. To paraphrase Latour, we can say that before Marx there was no class struggle, but after Marx it has been *always there*. Marx's theory informed various processes and practices of world making, it was literary engraved into real concrete objects and bodies. In other words the way of looking at the world also formed it, helped it to come into being. Even though there may not have been any real class struggle before Marx it became very real during the 20$^{th}$ century.

Law and Urry provide us also with other examples from economy; namely the application of game theory. Law with Urry describe the case of Ken Binmore, an economist and game theorist at London Bussiness School, who was asked by the British government to create set of rules in order to an auction of the frequency spectrum for mobile-phone operators. Binmore thus applied game theory to organize the auction and achieved on one hand respectful goal of raising £22bn for the government (instead of estimated £5bn); but on the other hand also raising a controversy whether the bidders were not over-charged thanks to their overall hype and the situation known in auction-theory as winners course (Law and Urry 2004, 394).

> Perhaps the problem was that though they used [the game theory] the bidders were not sufficiently proficient in applying [it]. If this is so, then the outcome of the auction can be understood as the intersection of more proficient uses of gaming theory [by the government] with less competent applications by some, at least, of the bidders. (Law and Urry 2004, 394)

Law's and Urry's example shows that the enacted reality cannot be an outcome of random theory being applied, nor is it fully determined by the scientific theory. Other factors also come into play, especially the resistance of other actors and their relations (2004, 396) in this

case the inadequate knowledge of the bidders. If the theory is not able to overcome such resistance, then it necessarily fails to bring worlds into being.[6]

This puts scientist (and basically everybody) in front of an important question: which worlds do we want to bring into being by our practices? According to Law and Urry scientific methods are never innocent (2004, 403; see also Haraway 1991c, 191; 1997, 191). Science, as an enactment of reality, engages in *ontological politics*; a form of politics in which the character of reality is decided and stabilized by particular processes and interactions. Basically reality is not *out there* as a matter of fact; it's rather a *way of being.*

While Law and Urry talk about ontological politics mainly in connection with social science, its theories and its methods, philosopher and anthropologist Annemarie Mol describe this term in wider context claiming that: "reality does not precede the mundane practices in which we interact with it, but is rather shaped within these practices." (Mol 1999, 75) In other words, science is only one kind of reality performing practice and even this one is not homogenous. Given the multiplicity of science methods and theories, we can also speak of multiple realities which these practices and methods of inquiry perform (Law and Urry 2004, 397).

The multiplicity of realities does not mean plurality. Such thought would lead to false image of separated distinct entities. Mol describes that multiple realities "are not simply opposed to, or outside, one another." (Mol 1999, 85)

> One [reality] may follow the other, stand in for the other, and, the most surprising image, one may include the other. This means that what is 'other' is also within. Alternative realities don't simply coexist side by side, but are also found inside one another. (Mol 1999, 85)

In other word we return to Latour's claim that reality emerges through interaction – here described as practice – and we can add that there can be multiple realities constructed through various interactions of multiple actors. My concern in this text is mainly about the human-technology interaction, therefore I will now move to the other key world making player – besides *science* – and that is the *technology*.

## b. Technology as world making practice

Technology is traditionally viewed as an extension of human body; a neutral tool which helps humans to achieve particular goals, most commonly to culture the world and maximize the use of resources (see White 2013 [1959]). However famous (and controversial) German philosopher Martin Heidegger describes technology as something that goes much deeper into our reality than just a mere tool; technology is for Heidegger a way of revealing, something that brings reality into being (Heidegger 1977, 12). Western technology for Heidegger changes how we perceive and interact with the world around us, thus it changes what the world really *is* to us. Thanks to technology world is turned into *bestand*; a standing reserve ready to be turned into resource (1977, 17). The greatest danger of technology is then for

[6] This is also described by Thomas S. Kuhn in his *Structure of scientific revolutions* (1975) as a crisis of normal science. When science meets with accumulation of controversies which it is no longer able to resolve with its tools, new scientific paradigm comes into place and with the change of paradigm comes hand in hand the change of a whole ontology of the world (1975, 111).

Heidegger that technology changes the entire essence of humanity; it turns the whole reality including humans into bestand (Heidegger 1977, 28; see also Verbeek 2005, 56).

Donna Haraway ds to this that this *bestandization* is co-produced also through science and practices of knowledge production:

> It - the world - must, in short, be objectified as thing, not as an agent; it must be matter for the self-formation of the only social being in the productions of knowledge, the human knower. […] Nature is only the raw material of culture, appropriated, preserved, enslaved, exalted, or otherwise made flexible for disposal by culture in the logic of capitalist colonialism. (Haraway 1991c, 198)

Thus the technology as being is embedded in modern science which establishes and naturalizes the division of world into subjects and objects.

Latour adds to this all-encompassing view of technology that technology can be viewed either as something neutral, just a technological mean to a human end – this point of view is best described by the slogan: Guns don't kill people! People do; or there is the other standpoint towards technology, that of technological determinism, in which technology is making people do things. (Latour 1994, 30-31) To put it simply in the former case the goals are only human and technology is just a tool how to achieve them; in the latter case the technology has some script of use and no matter who is using it, the technology determines the possible goal. Either there is a pre-given subject manipulating objects around him, or there is a pre-given subject manipulated by the objects.

These two opposing camps are according to Latour both wrong. Latour claims that if a person uses any technology (i.e. the gun) a new entity emerges with new goals. This is what Latour calls *translation;* translation is "displacement, drift, invention, mediation, the creation of a link that did not exist before and that to some degree modifies two elements or agents." (Latour 1994, 32)

Technology thus creates new ontologies emerging from interaction. There are no pure forms mingling together, there is no pure man(sic) enhanced with the pure gun, there is a gunman; a new entity with new goals and possibilities going beyond the goals and possibilities of the previous entities. What is important for Latour is symmetry in this approach, according to Latour we cannot say what comes first, whether the gun (technological determinism) or the man (subjectivism). The entity of gunman is not inseparable in terms that the gun would grow into man's hand, but if we separate the gun from the gunman, the gunman ceases to exist and yet again new entities emerge, that of a gun and of a man.

But in this account Latour only describes how technology relates to the individual and vice versa; they mutually change each other forming a new entity. But how does in Latour's view technology relate to society? And how it relates not to society as a sum of individuals, but how does it relate to society as a process, a way of being?

Latour argues that *technology is society made durable* (1990); respectively that society is turned into durable and stable whole through fabrics connecting human and non-human actors (Latour 1990, 103). Latour describes that in order to exercise power over other human actors it is possible not only to communicate intentions directly, but also develop durable alliances with non-human actors which have inscribed certain *program of action*; in other words these

actors invite particular type of interaction – i.e. the escalator going in one direction invites the pedestrians to use it only in this direction.

Nevertheless the program of action doesn't secure smooth compliance by itself (that would be technological determinism all over again). Latour explains that to form a durable whole the use plan has to be supported by other actors insisting on its following (Latour 1990, 109). In case of the escalator there also have to be signs prohibiting pedestrians from using it in the wrong way and eventually security guards supervising the smooth flow of passengers. The more actors are involved the lower is a probability of someone/thing enacting so-called *anti-program.*[7]

Anti-program is an improper use, an act of disobedience to the program of action. In our case it would be a person using the escalator in wrong direction; blocking the exit from the escalator or using the dividing strip between two escalators as a slide. The aim of technology is usually to prevent anti-programs from happening; that is also the reason we have nowadays various barriers on the dividing line between two escalators. The more anti-programs are prevented the more *predictable* becomes the behaviour of various actors (1990, 105).

Technologies may vary from simple tools such as wooden stick, to complex social technologies such as bureaucratic systems (see Graeber 2015), to even more complex socio-technical systems such as the internet. Each technology *translates* the actors in different ways and with different outcomes; each technology also has different use program and possible anti-programs.

Science and technology thus are two key actors in western ontology politics. Donna Haraway calls their merger fittingly the *technoscience* and "[w]e are inside its material grammar: we both embody and contest its rules." (Haraway 1997, xiv) The reality then is being enacted through "the knowledge-power processes that inscribe and materialize the world in some forms rather than others." (1997, 7) The ontology politics is thus the struggle over power to bring durable worlds into being; worlds which will mobilize enough actors to overcome resistance of others.

The questions concerning human ontology politics in technoscience can be approached through *cyborg anthropology* which "attempts to refigure provocatively the border relations among specific humans, other organisms, and machines," (Haraway 1997, 52) and "explor[es] the [co]production of humanness through machines." (Downey, Dumit, Williams 1995, 265)

The term cyborg entered the realm of social science mainly through works of Haraway (1989; 1991; 1997) and in her account it is a signifying boundary creature decentering the fabricated and then naturalized pure categories human, animal and technology (1991, 2; 1991b 152-53). Such concept presents for Haraway a way out of dualism through which we were interpreting humans and their technology (1991b, 181) and thus comes very helpful in imagining the new actors emerging out of interaction which Latour describes in his work. The point is that cyborg is indivisible, if we try to put some part away, it stops to exist as such and turns into something else.

Latour's account of the creation of objects/subjects is concerned mainly with very particular pieces of technology such as gun (1994) or keychain (1990). But what if we need to

[7] The supervision of program enactment does not concern only human but, also non-human actors, that is why many technologies have various kinds of fuses or safety-switches.

study the emergence of subjectivity in contact of actors in much larger scales such is the internet? For such a purpose British philosopher Timothy Morton introduces a term hyperobject.

### c. Hyperobject

Morton's ideas are also based on symmetrical Latourian metaphysics, where humans and non-humans act together. Nevertheless Morton besides ordinary particular objects, introduces also *hyperobjects* (2013, 1), entities which are too big to be grasped or even imagined in their entirety such as global warming, the sum of plastics, production machinery of capitalism (or surveillance machinery of state socialism). Unlike Giddens' abstract systems, hyperobjects are material *agents* (2013, 29); their intangibility is a problem of scale not of abstraction.

Hyperobjects have in common multiple features; they are *viscous,* which means they tend to stick to beings they are involved with. They are also *nonlocal*, thus what we can only see of hyperobjects are their mere *local manifestations,* but not hyperobjects themselves. Not only their spatiality, but also their temporality is beyond human scale, thus hyperobjects are at least partially occupying different time space than their parts. (ibid.) In this account Morton is drawing on Kant's separation of *noumenal* and *phenomenal* world. Because hyperobejcts are spatially and temporally ungraspable by our imagination to their full extent, they resemble the *noumena* while their manifestations are the only way how we can approach hyperobjects thus associating the *phenomena*. (2013, 11) Therefore Morton argues that "it seems like good practice to start with the things at hand and feel our way forward" (2013, 15) if we want to approach hyperobjects.

Moreover Morton's hyperobejcts change our notion of life and society (2013, 15) and shape other objects including our human *selves* by series of wounds and measures adopted to protect selves from such inscriptions (2013, 51). In other words hyperobjects symbolically and physically mark themselves into objects and bodies (2013, 54); they represent important actors in making other quasi-subjects/objects. Besides, in Morton's view also human (as a geophysical species) is a hyperobject; a hyperobject to produce other hyperobjects (Morton 2016, 45). From agriculture, to nature/culture, to Anthropocene, human also sticks to and inscribes itself into other bodies while creating new hyperobejcts which reciprocally inscribe themselves back into human.

Hyperobject, like any other quasi-object – is not ahistorical entity, it is not simply out there, it has to be crafted, negotiated a brought into being by various actors and practices. So how does the hyperobject actually differ?

Well given its scope and viscosity the hyperobject demands different kind of policy in order to be dealt with. Unlike object, hyperobject cannot be send *away* when unpleasable; the dealing with hyperobject cannot be delegated onto some other – whether this other is so-called *nature*, or the *third world* (Morton 2013, 109). Take pollution as an example; before pollution started being hyperobject – or what we now call global pollution – it was send *away* to other countries, other continents, other environments and those others were expected to take care of it (and often still are). But the hyperobject is like Ulrich Beck's *risk* (Beck 2011, 400-401), it does not copy the unequal distribution of wealth, it affects everybody. It is not democratic, it does not treat all the same, but everybody is somehow touched by the

hyperobject, the hyperobject sticks to things and the more we decide not to see it, the more it gets inscribed into other objects beyond our control.

Morton thus proposes to deal with hyperobjects differently not by trying to eliminate them – because that always means the sending *away* – but by coping with them *in-here*, controlling them and making their inscriptions less violent and more predictable. As an example Morton mentions the design of *Dusty Relief*: "an electrostatic building in Bangkok that would collect the dirt around it, rather than try to shuffle it somewhere else. Eventually the building would be coated with a gigantic fur coat of dirt." (Morton 2013, 109)

Likewise the global pollution, the ICTs respectively the *internet* belong among the human-made *hyperobjects.* The internet is very viscous; I remember how one of the speakers during a talk about state surveillance in Paralelní Polis [8]said that the only way how to be 100% sure, that we are not being followed on the internet, is not to use the internet at all and everybody laughed. This is how viscous internet is; it is so absurd to think about oneself off the ICT grid, that such a remark is automatically perceived as a joke.

Internet is also very non-local. Indeed its non-locality is internet's very fundament; we may say its *causa finalis*. Developed by the American army during 1970s as a communication system for military research, internet is a war child of the cold war (another hyperobject) threatening the world with nuclear annihilation. "The non-centralized structure of the [internet] was related to the need for it to survive nuclear destruction of component parts." (Haraway 1997, 4-5)

The quest for privacy then can be described as a resistance towards the inscriptions of internet. Since according to Floridi (2005, 195) objects (including selves) and information form indivisible whole, hence the struggle to control one's own informational privacy is the struggle to control the self. This already applied to the modern technologies such as photography, but increases in scope with the ICTs.

Even though Latour tears down the whole Cartesian dualism of subject/object it is extremely difficult and it might be even counterproductive to abandon this divide completely. Mainly because without this divide any question of privacy – if we use Barthes definition concerning ontological categories of subject/object – wouldn't be necessary.

If we follow Latour's line of thought the divide of subject/object disappears for us as for analysts, but it doesn't disappear for the actors themselves. The only thing is that (in Latour's terms) the divide ceases to be *matter of fact* and becomes *matter of concern*. What actors might call subject Latour describes as *quasi-subject*. Quasi-subjects consist of different actants such as bodies, legal documents, biographies and such, cooperating together in order to establish someone as a subject (Latour 2007, 208). Latour calls these actants *plug-ins* and different plug-ins establish according to him, different subjectivities. Therefore when is speak of subject in my analysis, I always mean quasi-subject. Both object and subject are two kinds of cyborgs. These cyborgs emerge from the coupling of a hyperobject with other actors to which it sticks. Thus a rainforest as hyperobject creates different cyborgs, than western technology.

[8] Paralelní Polis is think-tank in Prague, focusing on propagation of anarchocapitalism and new cryptocurrencies such as Bitcoin.

Moreover these subjects/objects are constantly renegotiated in particular interactions with multiple other actors. Beautiful example presents Eduardo Kohn in his acclaimed book *How forests think*, where he in the very beginning describes why his guide Juanicu warned him about his sleeping habits:

> "Sleep faceup! If a jaguar comes he'll see you can look back at him and he won't bother you. If you sleep facedown he'll think you're aicha [prey; lit., "meat" in Quichua] and he'll attack." (Kohn 2013, 1)

On this piece of advice Kohn describes how the change of position can turn him from equal subject into an unequal object (prey or meat) in the eyes of the Jaguar. The western human struggle for privacy in the infosphere is equally such pursuit of subjectivity in the eyes (or other receptors) of other actors. It is one's endeavor to maintain control over her information and not being turned into "meat".

### d. Rainforest as hyperobject

Even though it may seem inappropriate to compare internet and Amazonian rainforests – mainly because Kohn in his work doesn't concern technology and focuses mainly on animal non-human actors – Kohn's analysis is a great case study demonstrating the relation of selves and *hyperobjects* (although Kohn does not use this term). Kohn's *anthropology beyond human* is in "large part about learning to appreciate how the human is also the product of that which lies beyond human contexts," (Kohn 2013, 15) thus it shows how hyperobejcts are inscribed into quasi-subjects and in what way the former help to co-create the latter and vice versa.

Kohn's ecology of the Amazonian rainforest described as a web of semiosis in which all the actors emerge in mutual interaction (Kohn 2013, 42). Selves are products of this web of semiosis while they also become new starting points for new reading and interpretation of signs, therefore for future selves (Kohn 2013, 34). The human interpreter is in no way central to this web and she is only one particular part of it. In this fashion we can interpret the web of semiosis as a hyperobject which is complex and full of contradictions and the emerging selves are just the particular demonstrations of this hyperobject.

This construction and upkeep of selves gets in Kohn's account almost Heideggerian phenomenological dimension, when Kohn speaks about the growth and change of the self. For Kohn the process of change and growing is the reaction on the disruptions in the world. His claim is that the world's "habits we in-habit" tend to be invisible to us, in Heideggerian terms we may say that world is ready-to-hand, whereas when some surprising rupture comes, the world becomes present-at-hand, it reveals its otherness (Kohn 2013, 63). The reaction of self is then to change its habit and remake itself, even just temporarily, in order to become one with world again. That can be read as a form of resistance towards the hyperobjects unpredicted inscriptions. The already established properties of hyperobjects, are already inscribed into the material bodies, thus the bodies in-habit the habit of the hyperobject. Nevertheless when a new property of the hyperobject emerges, the *self* has to react by inscribing this reaction to the new property into itself, otherwise the hyperobject will inscribe the new property into the *self* by force, objectify it and change it against the *self's* will and mainly beyond the *self's* control.

In the case of internet we can see the reactions of the particulars to the changes of the hyperobject in terms of shifts in socio-technical systems such as operation programs. Software which is not up-to-date with operation programs must be rewritten, or will perish because of non-use. Similarly user who is not capable to react to the changes in the interface will sooner or later loose her access to certain areas. Needless to say that non-use is in no way abolishment of the connection between the hyperobject and the self. Donna Haraway puts it simply: "Ignoring social cues is far from neutral social behavior." (Haraway 2008, 24)

The Kohn's rainforest is thus a hyperobejcts creating its own cyborgs; only given the features of the forest the merger is not of humans and machines but of humans and animals (Kohn 2013, 107; Haraway 1991b, 152). By various practices the humans are trying either to unite with non-humans or to strengthen the division from them. That depends on what goals the Runa follow and what position they want to or rather can have in the hierarchy of interaction. For example if a Runa wants to attract prey or woman, he tries to join with anaconda, because "anaconda is a kind of predator that hunters would like to be: one that is not initially recognized as such." (Kohn 2013, 122) By analogy the same practices are used by various hackers and malwares to attract their *prey* which will be discussed further in the text.

On the other hand in other situations Runa engage in practices separating them form other beings, like when they try to discipline their dogs. When the Runa dog misbehaves, his owner has to talk to his human side, therefor he infuses the dog with drugs, but on the other hand he always uses special tense which is prescribed only to dogs, otherwise the Runa would be like a dog himself (Kohn 2011, 144). Similarly programs and human users on the internet engage in various practices how to distinguish one from each other; the most notoriously known example is the CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart") tool which is used by websites to separate humans from software.

## e. Infosphere as a hyperobject

Luciano Floridi calls the ecology consisting of information and communication technologies (ICTs) the *infosphere.* In his book *The Fourth Revolution* (2014) Floridi claims that the ICTs and their interconnectedness and omnipresence create completely new environment which shapes the reality of the world we live in by making it informational (2014, 40). His definition of infosphere is located between two points with various degree of intensity. Minimally the infosphere represents the sum of all informational entities and agents (2014, 41) thus the least definition of the infosphere treats it as a *hyperobject*. Maximally the infosphere is in Floridi's account treated precisely as the whole reality based on information (Ibid.), therefore we can also speak about infosphere as an *ontology*.

These two dimensions of infosphere are in mutual dependence and co-construction. Basically the viscosity of the hyperobject is enforced by the claim, that everything is reducible to information (Haraway 1991a, 62) and thus the hyperobject can stick to and consequently absorb any other reality (Floridi 2014, 44). As an example, Floridi provides the case of Radio Frequency Identification (RFID) chips being implemented into all kinds of entities including humans (2014, 45). These RFID identifiers enable various devices to identify, read and store information about the actors implemented with the chip.

Such chips and implants are supposed to provide more fluent and effective exchange of information between various actors, but they can also be actors in ruptures. For example when

I first entered Paralelní Polis one of the people introduced himself to me and offered me that I can scan his RFID implant in his hand and download his business card. Unfortunately I am not the kind of cyborg able to do that, simply because I don't (intentionally) own a smartphone, which would be able to read the chip. In other words the hyperobject of infosphere didn't stick to me or rather inscribe into me as was expected, which in the final effect excluded me from a certain type of technologically mediated interaction. On the other hand my obsolescence stemming from my old V-type mobile phone raised curiosity in some members of PP and engaged them to further communication. On one hand it made me an outsider for particular activities; on the other hand it made me look exotic because such kinds of cyborgs are nowadays not that common in my generation and socio-economic class. In the end the RFID implanted man was partially disappointed because he couldn't demonstrate the abilities of his own cyborg body but also partially excited to meet a different kind of techno-scientific species about which he thought slowly disappeared, at least in these parts of the world.[9] In Haraway's words I became a boundary creature – a monster – and "monsters signify". (Haraway 1991, 3)

This example demonstrates how ICTs in the infosphere nowadays cannot stand for themselves. Every particular technology is a part of bigger mutually interconnects sociotechnical systems based on norms and negotiations. This network of various actors needs their full cooperation in order to work properly; the ICTs are thus mutually influencing each other and can hardly perform on their own without the support of their counterparts. As such ICTs are part of the hyperobject infosphere which shapes them, but also is essentially depending on them. Without unified infosphere the ICTs would not perform, but without performing ICTs there wouldn't be any infosphere.

But the infosphere is producing individuals also in other, deeper ways than just in material merging of bodies and technology. Actually Floridi calls ICTs "the most powerful *technologies of the self* o which we have been exposed." (2014, 59; emphasis in original) That is because ICTs create the ecosystem through which flow the information one is gaining and also producing (2014, 60-61). If we borrow concepts from some other hyperobject such as the Amazonian rain forest, we can conclude that particular selves are always an outcome of specific webs of meaning which surround them (Kohn 2013, 42).

Hyperobjects present such webs of meaning. The difference of those two hyperobjects is not in their natural/artificial dimensions. Those are only classification shortcuts manufactured to separate actors and enable the establishment of modern subject/object divide. But in the technoscience we were born kin to the infosphere (Haraway 1997, 62) in the same way as Runa people are kin to the jaguars within the forest (Kohn 2013, 107).

That is because infosphere as ontology is also being enacted by various actors. American philosopher N. Kathrine Hayeles comprehends the root of this informational ontology in the Macy's conference on *cybernetics* (Hayles 2008, 50)**.** Similarly as the Runa people see and perform everything in the forest as a potential human self (De Castro 1998, 470; Kohn 2013, 17) western technoscience tends to interpret reality in terms of information. Haraway argues

[9] Susan Leigh Star (1990) describes similar situation when her allergy to onions shows how she does not fit into pre-scribing categories.

that "we are living through a movement from an organic industrial society to polymorphous information system," (Haraway 1991b, 161) and ads that:

> Biological organisms have become biotic systems, communications devices like others. There is no fundamental, ontological separation in our formal knowledge of machine and organism, of technical and organic. (Haraway 1991b, 177-78)

What started as an analytical direction trying to grasp reality in innovative way in fact enacted such a reality and brought it into being.

Thus the infosphere as *hyperobject* and as *ontology* are mutually co-shaped through practice, enactment and embodiment. In Hayle's words "embodiment mediates between technology and discourse by creating new experimental frameworks […]." (Hayles 1993, 163) That is for infosphere as hyperobject does not act by itself, it is not a cause of things; it is a mediator. The hyperobject translates interactions and relations between various actors and thus creates new ones. Similarly as in Latour's example a gunman – as new ontological entity – emerges from the merger of gun and man, the cyborg in the infosphere emerges through his contact with the hyperobject.

Extent of the overall success of this reality enactment was clearly visible in the *Big Bang Data* exhibition which took place in Prague during spring 2017. The exhibit maps different dimensions of so-called datafication. It shows how the infosphere gets inscribed into more and more objects varying from human bodies, to animals, to plants, to ocean waves. At the same time it captures the incredible scale of data produced in one day creating an overwhelming cacophony of pictures, words, contacts and reports. Expanding in incredible numbers creating overwhelming noise the data indeed seem to be exploding and creating a new universe, a new Big Bang.

But this didn't come from nothing and such hyperobject has its history. That history starts with cybernetics of Gregory Bateson, Allan Turing, Norbert Weiner and others and continues till this day because we started to create inscription devices – mainly computers – which helped us to turn surrounding objects into information, give them the informational value of ones and zeros. Despite the overpowering feeling datafication lays upon individuals, we have to remember that there are still multiple objects resisting such reality, including human mind and emotions.[10]

Nevertheless, given its great scope, the infosphere as a hyperobject connects multitude of various actors. In order to do so there has to be some objects plastic and flexible enough so they can connect actors which fundamentally differ and *translate* them therefore those actors can effectively interact with each other. Susan L. Star with James Griesemer (1989) call such objects *boundary objects*. Boundary objects are such "objects which inhabit several intersecting worlds and satisfy informational requirements of each of them." (1989, 393) These objects are further "plastic enough to adapt to local needs, yet robust enough to maintain common identity across sites." (Ibid.) Such objects in the infosphere are the computational devices with their user friendly interfaces. These devices are able to translate the language of infosphere into human language and equally, they can also translate human

[10] Despite some authors believe that the invention of artificial intelligence is just a question of time (i.e. Kurzweil 2005) others claim that such a belief is mistaken and that human brain is not reducible into a computer (Epstein 2016).

practices into computational language and communicate it with other non-human actors in the grid.

## f. Infosphere and production of self

Despite the general belief of unlimited possibilities of cyberspace, we are not free to design whatever identity we would like to adopt in the infosphere; those were the dreams of the early 90s (Floridi 2014, 64). But the idea of complete disembodiment in the cyberspace showed repeatedly wrong through the end of second millennium (Hayles 1993, 149; Muri 2003, 77; Rey & Boesel 2014, 173). According to Floridi online and offline identity has to coexist in the equilibrium of so called *onlife* (Floridi 2014, 73). Yet there are still virtual environments where this is not so strict, as an example may serve the cases of second life, where people develop multiple identities completely differing from their offline selves like "a man playing a woman who is pretending to be a man." (Turkle 1997, 73) But even those identities are not completely independent on the offline ones. As one of Turkle's informants further elaborates, these identities, the alternative selves, allow him to talk about topics he wouldn't be able to talk about in his own self (Turkle 1997, 79). Jenifer Cool goes even further on this mutual dependency of online and offline identities and practices by claiming that "[…] online practices express [offline] social relations, albeit in complexly reconfigured and reconfigurable forms." (2012, 24) That means that the social identities we develop and maintain are also affected by the technologies we use and their design, no matter whether these identities first appear online or offline, they are usually affected and co-shaped by the ICTs as technological mediators.

P.J. Rey and W. E. Boesel (2014) argue that even the dualism of online and offline is inherently wrong. They develop this argument on Derrida's statement that the purpose of constructing binary categories is always to make a value judgement (Derrida 1982, c.f. Rey & Boesel 2014, 179); hence one is always constructed as superior to the other. In this case the aim, according, to the authors is to "devaluate digitally mediated experiences" (2014, 173). To avoid this dualism Rey and Boesel speak about *augmented reality* (2014, 178) which is according to them producing *augmented subjectivity* (2014, 184).

The augmented subjectivity is carried out through embodiment of our physical bodies simultaneously with our digital prostheses, whether these are our mobile phones or Facebook profiles (Rey & Boesel 2014, 173). This is basically how the infosphere as a hyperobject inscribes itself into us, because "our interactions with and through [ICTs] are constantly shaping our choices of which actions to take." (2014, 178)

This is exactly the reason why cyborg anthropology seems as the right approach to better understand current western culture. Floridi claims that we understand ourselves as cyborgs not through technological enhancement of the body with implants but because we radically transformed the environment in which we live (2014, 96). Sherry Turkle than further develops on this idea by stating that various device we use aim to help us to orient in this increasingly complex informational environment. They become so crucial that we basically develop new selves with them to the extent that we almost *become our devices* (Turkle 2011, 151-152).

On the other hand the devices, even though they present crucial interfaces translating the digital code of the infosphere, would be obsolete without the data. With the emergence of cloud storages it may be even said that particular devices are not crucial to the user, because

her data can be accessed with any device of particular kind by using the right password. Thus the shift in perspective to current cyborgs is not caused by the mere use ICTs but rather in the change of ontology, turning the world of matter into the world of information flow (Floridi 2014, 97).

The data which we daily produce and which surround us; create according to Deborah Lupton (2016) something that Donna Haraway calls *companion species*. This also means that the data assemblages we are entangled with have life of their own partially beyond our complete control. (Lupton 2016, 3; Turkle 2012, 160) In Haraway's account the cyborg or companion species are figures which represent material semiotic knots where "diverse meanings and bodies co-shape one another. [These] figures are at the same time creatures of imagined possibility and creatures of fierce and ordinary reality." (Haraway 2008, 4)

## g. Privacy as ontological border

Crucial in the process of self-making is the labour of division (Watson 1997, 151), which distinguishes the self from the other. These acts of division have been subject of many debates in social and cultural anthropology. Anthropologists Marry Douglas (2001 [1966], 2003 [1970]) and Judith Okely (1983) conceptualize the border of the body as a symbol for the border of the group. Purity of the subject symbolizes the purity of the group formation and prevents an alien entity from penetrating the subject hence the group. The boundary work has in their terms symbolic social function. The pure coherent subject's body serves as a structure for understanding of broader complex social systems (Douglas 2001, 116).

But if we accept Latour's claim that all the subjects are quasi-subjects co-constructed through multiple entities, the border work which has to be performed and is called privacy is basically managing the border controlling which actors are being let into the assemblage of quasi-subject and which are not. This sieving is done by various actors including humans themselves. Haraway claims that "the tradition of reproduction of the self from the reflections of the other – the relation between organism and machine has been a *border war*. The stakes in the border war have been the territories of production, reproduction, and imagination." (Haraway 1991b, 150; emphasis added)

I draw my notion of this division mainly on Donna Haraway's work about the *Constitution of Self in Immune System Discourse* (1991d). For Haraway the biological self in 20th century is semiotic system of *recognition/misrecognition* and any disease "is a subspecies of information malfunction or communications pathology; disease is a process of misrecognition or transgression of the boundaries of a strategic assemblage called self." (1991d, 211-212)

For the ontological difference between humans and their machines in technoscience is basically absent (Haraway 1991b, 152) the case with self in the infosphere is the same. That is because both the human mind and body are according to Haraway reduced to the flows of information (1991b, 164-165) and the infosphere can be viewed as a technology designed to effectively mimic those two dependent dimensions of human existence. This can be well demonstrated on the case of the *virus,* an entity attacking both biotic and ICT systems.[11] Both

[11] The Virus is not the only entity which is in technoscientific imagination common for biotic and artificial systems. Techno-futurists such as Ray Kurzweil (2012) and Hans Moravec (1988) are in their (highly questionable) works proposing that even the human mind works as a computer. On more serious note, Stefan

kinds of the system then also need *healing* no matter whether we talk about biological bodies or computers.

The main entry point for the other into the self are the *boundary objects,* hence the interfaces and devices in the infosphere. Therefore these are the main points over which there is the struggle for control. "One should expect control strategies to concentrate on boundary conditions and interfaces, on rates of flow across boundaries, not on the integrity of natural objects." (Haraway 1991d, 212) The boundary objects are the knots through which the flow occurs and thus these are the ones which must be regulated and maintained in order to stabilize subject/object in the infosphere. In other words, who can control the boundary object becomes the actor which can re-define the ontological status of other actors. That is why users aim to protect their devices (boundary objects) while intruders are trying to seize them, no matter whether these intruders are states, corporations or criminals.

The protection of boundary objects is carried out by so-called *labor of division* that can be performed by human or non-human actors, and according to anthropologist Morten A. Pedersen it represents also a form of connection (2014, 203). Pedersen analysed practical application of the magical gown among Northern Mongolian shamans and half-shamans (shaman apprentices) and concluded that this particular object is used in order to detach the user from the realm of spirits; basically to establish a safe distance between particular humans and particular non-human divine entities (Pedersen 2014, 200). The magic gown serves as mediating object which enables the owner to be "neither too shamanic nor too little shamanic" (Pedersen 2011, 179); it mediates relation through division (2014, 205).

Pedersen's analysis comes handy to the analysis of infosphere because the experience of half-shamans with spirit realm surprisingly reminds the western experience with the infosphere:

> For although it is true that the shaman is made able to enter the realm of the spirits by donning the gown (which is what the literature on shamanism usually focuses on), it is also true that she, ipso facto, also becomes able not to see the spirits (*and not to be seen by them*) by taking it off. This ability opposes to that of the 'half-shamans' who, for lack of ways of blocking the paths of the spirits, are exposed to them all the time, without being able to see them, let alone control them. (Pedersen 2014, 201; emphasis added)

The difference between shamans and half-shamans bears reminiscence with the difference between ICT professionals and lay users. Whereas the professionals are able to see behind the interfaces of the infosphere and their movement in it is instinctive and almost embodied, the lay users lack those abilities. Their interaction with the infosphere is way more asymmetrical for their deficiency of knowledge and skills; the lay users are *exposed* to the infosphere beyond their control.

And similarly as the magic gown keeps safe distance between the human and non-human selves, we use and mobilize lots of actors and practices in order to establish safe distance between our informational selves and the rest of the infosphere. Haraway reminds us that individuality is based on strategies of control and that such job is delegated on various *non-selves* which to the self may seem alien and weird (1991d, 222); to put it briefly the cyborg

---

Helmreich analysed in his book *Silicon Second Nature* (1998) group of computer scientists culturing artificial life in the software environment. This approach of evolutionary algorithms has nowadays main application in entertainment industry.

self is in no way an aesthetically pleasing and fully coherent entity. It takes multiple forms which may co-exist in one moment and contradict each other at the same time (1991b, 155).

In this text I will further analyse various types of non-human actors to which the labour of division is delegated such as Bitcoin, ad-block, or anti-virus. All these virtual objects are designed in order to protect different kinds of privacy from different (but interconnected) intruders. In this way each of these actors co-creates multiple subjectivities with its own diverse politics. Furthermore these subjectivities are not mutually exclusive; they can be part of one assemblage completing a quasi-subject.

## 4. Talks with John Doe

During my research I've met John Doe, who became my informer. On various occasions John Doe appeared to be a hacktivist, a bitcoin user, a university employee mining profiles of alumni from linked-in, a fellow student or a guy who likes to dig dirt online on his divorced aunt whom he hates sincerely.

John Doe is not one person, he consist of 5 different people, all males between 20 and 40. Usually those were people that I've met during my participatory observations on various talks and conferences concerned with the topic of informational privacy or colleagues who showed interest in my research topic and had some experience with ICTs and/or privacy protection on which they were able and willing to elaborate. People who see behind the interface of ICTs which surround us and which present to the lay user one way mirror. In order to protect their privacy and anonymity I decided to create a shared identity.

### a. John Doe and the Internet

John Doe is a figure used in US courts, precisely in the lawsuits against anonymous defendants filled by large corporations (Lidsky 2000, 857; Lidsky 2009, 1373-75). Johns/Janes Does were usually internet users who spoke their mind on the web and were sued for libel. Interestingly those *John Doe cases* were filled by large companies not to gain financial recovery, because John Does usually don't have big financial resources or libel insurance; those suits were actually symbolic filled in order to silence the anonymous internet users (Lidsky 2000, 859-861). According to Lyrissa B. Lidsky "these Internet defamation actions threaten not only to deter the individual who is sued from speaking out, but also to encourage undue self-censorship among the other John Does who frequent Internet discussion fora." (2000, 861)

John Doe is thus the anonymous identity in the infosphere over which various agents battled to be able to control it. The John Doe cases brought attention to the right to speak anonymously on the internet (Lidsky 2009, 1376). To support this right I pay tribute by calling my informers the same name that was used for the anonymous users.

### b. John Doe as a strategy

In my case *John Doe* is not a legal but rather a literary figure, which highlights the importance of privacy on the Internet. I use it because my informers has the similar goals and motivations in their privacy oriented practices, that is to protect their right to control their identity, nevertheless their strategies to achieve this goal may differ. I find John Doe useful to create this shared heterogeneous identity of a privacy protector who is *neither one nor many.* Every

time I spoke with someone concerned with privacy I spoke with John Doe in a particular occasion. I even have a photograph with John Doe (see figure 1) which quite well illustrates the contradicting nature of his identity. It is a photograph of me and one of my informers wearing a mask of Guy Fawkes popularized by the graphic novel *V is for Vendetta* by Allan Moore. Thanks to the popularity of *Anonymous* hacktivist movement, this mask is widespread as a symbol of cyber-resistance. It helps to enact the *shared identity*, which is a strategy used by various rebel groups from Spartacus (or rather his Hollywood depiction) to Luther Blisset (Brunton and Nissenbaum 2015, 15-16; Deseriis 2012, 140-141). This strategy is so widespread that over the years it became "almost a *cliché*" (Brunton and Nissenbaum 2015, 15-16).

Marco Deseriis (2012) calls this strategy the *improper names* which he defines as "a radical form of subjectivity" which "challenges the modern state's invention of the legal name as a political technology of individuation." (2012, 157) The improper name functions as a strategy for sustaining anonymity and yet gaining recognition as a subject and not being dissolved in objectified anonymous mass. (2012, 152).

Given the claim of John Law and John Urry (2003) that by the way social scientists write and construct their theories, they bring realities into being, I am trying to bring the reality of John Doe into being and let this shared subjectivity of improper names to emerge. Even though none of my informers inscribed the identity of John Doe explicitly to themselves, they all are concerned with their personal space and they actively resist their objectification in the hyperobject-infosphere to be inscribed into their identities. By their willingness to share with me his strategies John Doe helped me to establish the boundary of private space as I now perceive it and as I analyze it in this text.

Therefore I don't' see John Doe as an informer, rather I see him as guide through environment which I was not completely familiar with despite my constant presence in it. Through my interviews with John Doe and through his insights, comments and practices I was able to establish an anthropological field out of my everyday reality; out of mundane objects and practices I come to interact with in my daily life. That has consequentially one almost absurd effect which I believe is typical for any research concerning ontology politics and cyborg anthropology: it seems like there is no way back. I could ask similarly as Octavia Butler in her novel *Dawn:* "I suppose I could think of this as fieldwork – but how the hell do I get out of the field?"' (Butler 1987, 91, c.f. Haraway 1991d, 230). Haraway then offers me with quite simple answer: "From this field of differences, replete with the promises and terrors of cyborg embodiments and situated knowledges, *there is no exit*." (1991d, 230; emphasis added)

### c. Secondary sources

The secondary sources that I worked with during my research were usually internet articles, movies, software or artistic projects connected with the issues to which directed me John Doe himself during our talks, or which he even published himself on his multiple blogs or other media. I chose these cases because they very well illustrate my conclusions and help me to demonstrate how these conclusions could be applied into future research.

I wasn't able to approach the selection of this data in any systematic manner, rather my approach was kind of Feyerabendian, meaning "everything goes". Paul Feyerabend in his

work about anarchist epistemology allows such things as accidental encounters to enter the scientific inquiry (1993, 252), therefore I tried to make myself more open and sensitive to such accidental encounters. This does not mean that I collect resources in some willy-nilly way, rather I try to turn myself into a scientific measurement device which is bombarded by the omnipresent manifestations of infosphere and at the same time decide whether these manifestations relate to the phenomena I chose to study, thus to informational privacy. My aim is to collect examples on which I am able to further elaborate my conclusions and to express various theoretical and ethical concerns related to my topic.

I usually chose objects depicting a controversy in the infosphere and its relation to informational privacy. As Latour suggests when uncovering the agencies of actors in forming hyperobejcts one should focus on moments of rupture which can be visible in several different ways; namely in innovations, accidents or breakdowns, but also resources of fiction, objects of art such as movies or installations (Latour 2007, 80-82). All these things can and often do signify the actors active in the de/stabilizing process of enacting the reality.[12]

## d. Personal shortcomings

It must be noted that I am not trying to present a complete picture of informational privacy in the infosphere. First I am not sure that is even possible at such complex topic, second I (involuntarily) participate in reproduction of particular oppressive realities.

The greatest shortcoming of my work is that I employed as John Does only male informers, thus I partially reproduce the view from nowhere trope in production of science. Given that my self is formed of male, hetero-sexual body which is empowered to make claims on so called objectivity.

> This is the gaze that mythically inscribes all the marked bodies, that makes the unmarked category claim the power to see and not be seen, to represent while escaping representation. (Haraway 1991c, 188)

I am part of such unmarked category, and this text fails to address the particular experiences of other marked bodies in the infosphere. I'm talking about women, homosexuals, people of colour and others form the underprivileged margins. Even though I borrow some examples from their experience, I don't analyse and address their problems in the infosphere. I use them mainly because these *boundary categories* (Haraway 1991, 3) signify the actors deployed in the processes of self-assembling even more, then the *mythical* uninscribed heteronormative male subject.

I am aware that the experience of subjectivity inscribed into these marginalized bodies will certainly differ from the experience that I describe in this text. And I hope that this text will help to develop a theoretical framework from which these situated experiences could be addressed in the future.

[12] Even this whole work is a process of negotiations which happens in instant struggle between my expectations and the manifestations of infosphere approaching me through various actors. My research is basically constantly reinvented and the final work is an attempt to stabilize it by mobilizing the actors that are available. This shall ideally make the text durable enough so it would survive the arguments of critical readers until the defense in front of the commission.

## 5. Politics of privacy

John Doe on one occasion told me that the main reason why he is protecting his privacy is because he doesn't want to be reduced to an object. He realized this when he was working for one big European university and was extracting information from the career oriented social network LinkedIn about the university's alumni:

> We don't know who the person in the profile is; we can only interpret the fake representation this person has put up. […] This made me realize that I don't want to be interpreted in this way; I want to be interpreted as the person who I am in the real world. That's why I started taking down some stuff from the internet. I became aware of how people see me and how I wanted to be seen. (John Doe, January 2017)

Here it is clearly visible that John's concern about privacy and representation is the same as in the Barthes' definition, thus the struggle to remain subject and ability to at least partially control the picture of himself. For John this is the case because various actors are trying to be able to predict the behaviour of users. And the ability of prediction is always based on certain level of objectification.[13] In general the problems of privacy in infosphere are very similar to problems of predation in Kohn's rain forest: "Predation points to the difficulties involved when *selves become objects or treat other selves as objects* within an ecology of selves." (Kohn 2013, 119 emphasis added)

John Doe interprets necessity of resistance towards informational predation while using a metaphor of medieval castle:

> The technology of thick medieval walls was a barrier developed to protect the castle against heavy canons. Where there is possibility to attack, there has to be some barrier against it. And that always cost resources. It is costly and difficult to build a medieval wall right? So even us in order to protect ourselves against technologies we have to spend resources to build systems which will protect us by its design. (John Doe, April 2017)

John also in another occasion reminded me that when we ask about the nature of privacy and the practices of intruders, we must not forget the form of object the intruders are trying to construct in order to achieve their goals. Different intruders need to create different objects. Based on the intruders' practices and their aims we can distinguish three different types: the *overseers*, *traders* and *criminals*.

Generally the *overseers* are concerned with control of individuals and their behaviour. Most notable overseers are states and information agencies, but overseers could be also employers or other institutions having access to the digital infrastructure. The overseers' goal is to perform power.

On the other hand, the *traders* are not concerned into reducing the subject into individualised object, but rather they need to classify the subject into particular demographics, with the purpose of effective advertisement. The traders are usually providers of some digital services such as Google, or Facebook, who has direct access to user's data. Traders then can bundle these data into big packets based on the demographic groups of the users and sell access to those data to other companies commonly with the purpose of targeted ads. Traders'

[13] Science is great example of such process, for science has to reduce phenomena into *scientific object* to be able to predict its behaviour in the future.

goal is to capitalize information and use it as a valuable asset; thus those are the key players in data driven economy.

*Criminals* are those intruders who operate outside the legal framework or violate the rules of use, typically referred to as hackers. Their aims may vary from trying to gain access to intimate information, to abducting users' computer and use it for other attacks or spreading the malicious content. Depending on their goals, also vary their victims from individuals, to companies and states (see Coleman 2014).

Those three figures are just ideal types and there is no clear boundary between these groups in terms of who can fulfil which role; on the contrary their goals and practices use to be closely interlinked. For example traders often sell their assets to political actors; two most current cases both involve the company Cambridge Analytica which provided the Big Data based digital campaigning for Donald Trump in US presidential election and for the pro-Brexit movement in Great Britain (Grassegger & Krogerus 2017). On the other hand i.e. Google spend lots of their financial resources on support of Obama's administration which was then in return very helpful in writing new "digital laws" and avoiding anti-trust charges (Wyatt 2013). And even the criminals are probably not independent on state; we can remember the hacking attacks targeting Hilary Clinton during her run for presidency in 2016, which were allegedly carried out by Russian secret services (Ackerman & Thielman 2016). Therefore also the various kinds of protection against various intrusions cannot be fully distinguished and they are described merely as ideal types; in practice the strategies of maintaining privacy usually overlap creating a multiplicity which is *neither one nor many*.

## a. Traders

Traders are the big information companies and data brokers who sell and trade personal data for profit (Mai 2016, 192). One of the nowadays almost text-book examples of the traders' intrusion of informational privacy is the so-called *Target case.* The target case became publicly known thanks to the 2012 New York Times article *How Companies Learn Your Secrets* by Charles Duhigg. Duhigg covered a story about a father who accused Target of inappropriate advertisements aiming on his 15 year old daughter:

> "My daughter got this in the mail!" [the father] said. "She's still in high school, and you're sending her coupons for baby clothes and cribs? Are you trying to encourage her to get pregnant?" (Duhigg 2012)

But later it was shown that Target sends these coupons based on the standardized customer behaviour indicating pregnancy and including buying higher amounts of lotion, minerals and other food supplements. Long story short, the girl was indeed pregnant, but she hadn't told her parents yet and the Target ad basically snitched on her. This case very nicely illustrates how various corporations aim on different demographic groups and thanks to their access to large datasets (big data) enable those to discover and "predict" or rather prescribe patterns in consumer behaviour.

### i. Objects as currency

At this point the products of the data tracking, hence the personal data traces of the users become new currency for various actors in the infosphere. Most of the services provided in the infosphere today rely heavily on the incomes from advertisements and thus the number of

users they are able to reach and the preciseness with which they are able to reach them become their most valuable asset (Floridi 2014, 50-51). John Doe commented on this topic that the use of those services is basically not free, but the users, instead of money, pay with their personal information. British *The Economist* claims that data harvested by companies such as Facebook, or Google are new *oil*, hence these digital companies are nowadays more powerful and richer than oil companies and other international giants (The Economist 2017).

This kind of privacy economy reminds the situation described by Warren and Brandeis back in 1890, but thanks to the viscosity of the hyperobject infosphere it is nowadays affecting way larger number of individuals and in different manner. Back in the 1890s the privacy related issues concerned mainly the upper classes, because those were the most exposed, thanks to current technologies and entrepreneurships; a *few* was exposed for the joy of *many*. Nevertheless in recent days it is the *many* that are being exposed to the *few*.

However the objectifying practices of market actors in the infosphere include not only collection of information, but also a distribution of specific information. Based on the collected data and demographic classification the companies show users in particular demographic group (i.e. pregnant women) specific advertisements based on their previous behaviour and purchases. The problem is therefore not just the collection of data, but also its processing (Mai 2016, 192).

John Doe argues that some people may actually like that the internet companies are showing them what they want to see, that the personalized advertisements based on their demographics are in fact beneficial for them:

> It is important to know who your customers are; if you want to fulfil requirements of your customers, you have to know a lot about them. In this sense it is useful for customers to disclose their personal information [to service providers]. (John Doe, April 2017)

On the other hand American/Dutch philosopher of technology Nolen Gertz argues that these advertising technologies are striping humans off their autonomy by manipulating users (2016, 59). Particularly the traders try to turn the cyborgs in the infosphere into objects in multiple ways; one is reducing them into mere demographic representors based on their statistically analysed behaviour; second is striping the audience off their opportunities to autonomously decide and delegate the decision process on the technology itself. Gertz calls this delegation of decision processes on non-human actors a form of nihilism when various service providers such as *Netflix, Spotify* or *Amazon* can through their algorithms prescribe our habits of consumption (2017).

These effects of technology on human autonomy are very well parodied in one of the episodes of famous satirical TV series *South Park* appropriately called *Sponsored Content*. The main characters of the show are repeatedly trying to find certain information on the internet and thanks to the in-browser advertising they always end-up eating ice-cream in a shop with a total blank about how did they get there or what were they doing in the first place. This satirical hyperbole illustrates quite well the experience which was described to me also by multiple friends of mine; namely the moment when they get lost in the infosphere,

because they click on random click-baits out of pure curiosity, while losing track of time and ending in unexpected corners of the internet.[14]

## ii. Cutting the chain

As I already mentioned, among the people criticizing the state and corporate surveillance practices in the infosphere, the option of non-use was automatically considered a joke and in the next part considering the overseers I will demonstrate why opting out of the infosphere is hardly an option.

It actually reminds me the situation from Luis Buñuel famous 1962 movie *The Exterminating Angel.* In this movie, a group of people spends several weeks in one room unable to leave it for no particular reason; even though there is no physical restraint, no door or threat whatsoever the idea of leaving the room seems absurd and impossible while necessary and appealing at the same time. Albeit the Buñuel's movie is a surrealistic metaphor rather criticizing certain rituals of higher society, the human relationship with the infosphere at some moments reminds the feeling of the people being trapped without any particular restraints or consequences in sight. Some people even claim that they feel we are suing ICTs too much, but quite ironically they express this feeling via sharing satirical pictures on Facebook. Al those criticizing people could leave, but at the same time it seems absurd and costly; the opting out brings too many unknowns, too many risks with it, the viscosity of the hyperobject is too high and it already stuck to too many things.

One of other options how to avoid intrusion of privacy from corporations I would like to discuss is establishment of private zone where the quasi-subject can be protected from their direct influence; in other words, avoiding the ads. To this purpose there are several tools usually called adblocks. The most notoriously known is probably the Adblock plus first developed in 2006 by Wladimir Palan for the Mozilla Firefox browser.

Adblock is what we may call an *opt-out mechanism* (Popescu and Baruh 2013, 275). But in this case the opt-out mechanism provides different mode of opting out than hiding personal information form traders. While hiding information from traders is basically controlling the information flowing *into* infosphere, the adblock protects the user from unvented information flowing in *from* the infosphere. It allows the audience, hence the quasi-subjects in the infosphere, to decide which content do they want to see while browsing the Internet. With this tool the users can filter out the unwanted advertisement in order improve their browsing experience.

While it is difficult to avoid the first mode of objectification without costs and repercussions, at least the users can avoid quite simply the second mode of objectification and at least in certain parts of the infosphere lower the influence on their decision-making processes. In this sense the adblock represents subjectifying actor by hiding from its users content encouraging specific consumer behaviour.

In this sense the ad-block is a different kind of dividing object than the aforementioned Shaman gown, because unlike the gown the adblock does not hide the subjects from the view of the infosphere at all, the adblock-ed subject remains visible to the corporate actors. But the

[14] It should be noted that this happens to my friends usually while being drunk and searching for music videos on YouTube ending up watching videos of "epic fails" or other curiosities, but the recommendations of YouTube videos work on the same principle.

ad-block (partially) protects the subject from their influence by cutting one of their most important communication channels with the users. Adblock as an actor reduces the flow of information in the opposite direction by maintenance of the interface hence the boundary object.

Another tool mediating the flow of information from user to the provider of service is for example the *Data selfie.* This plug-in works only for Google Chrome browser and it does not directly prevent any information from being exposed, it only provides its user with the list of information that the user shared with Facebook. Such device doesn't protect the user form privacy breach directly, but it clearly visualises the kinds of data that are shared by the user which helps to establish more symmetrical (but not equal) relationship between the user and the provider of the service. It helps the user to gain more control on the information flow through the boundary object (interface of Facebook). If we say that our privacy is what we pay for use of a service, plug-ins like *My data selfie* print us the receipt, so we can check our spending.

Only after few hours of using the Data selfie I discovered about myself that in the "eyes" of Facebook I am:

- *Likely to*: eat out frequently (even though I don't do that)
- *Not likely to*: have a gym membership (despite I have one)
- *Not likely to*: like outdoor activities (actually love camping)
- *Not likely to*: be concerned about the environment (I am concerned, but it is true that I am not very active)
- *Not likely to*: consider starting a business in next few years (this one seems actually completely true)

Besides that I was offered a clear view of my *big five* personality traits[15] or supposed shopping preferences, according to which I am for example *likely to* be influenced by online ads and social media when buying products, *not likely to* be influenced by brand name or product utility when making purchases or that I am probably not easily influenced by family members while shopping and that I tend to make "spur of the moment purchases". Those are just a few of the statistics and characterizations that Data selfie offered me base on roughly 16 hours of use.[16] The other characteristics included my psychological gender, intelligence, life satisfaction or religious and political orientation.

The data selfie allows me at least partially see what kind of object is Facebook able to construct out of my behaviour in its environment. Since the moment I first installed this feature I realized how I discipline myself differently because I started more consciously choose what I was looking at, in order to put together representation of myself which would more fit my tastes. I was simply trying to create a picture of myself which I would find appealing.

This self-discipline is similar to practices of self-tracking or life-logging, when people use wearable devices in order to reflect more effectively on their body. ""The body/self as it is produced through self-tracking, […], is both subject and product of scientific measurement

[15] Five categories used in psychology including Extraversion, Emotional stability, Agreeableness, Conscientiousness, and Culture (Barrick and Mount 1991, 2).

[16] I would like to use the Data selfie plug-in longer, but unfortunately it is currently compatible only with Google Chrome browser whereas I use Mozilla Firefox which supports more plug-ins for my everyday use.

and interpretation." (Lupton 2014, 6) In certain sense these technologically mediated practices does not prevent one from becoming an object, but it allows her to more consciously participate in the final shape of such object.

### iii. Summary

The traders create out of personal data an object of exchange. Their aim is to commodify user's behaviour in the infosphere and thus create possibilities to predict and prescribe certain modes of consumerist behaviour over others. The traders accomplish this goal through reduction of the user into demographical categories which help the traders to sell these objects as commodity.

Modes of resistance may vary. One way how to avoid objectification from traders is to opt out from their services, but that generates new problems which I will discuss in next chapter. Other safer way, is to reduce the direct influence of traders on the user, by blocking their channels of communication in the boundary object. This practice does not prevent the commodification of user, but it partially protects the user from being exposed to targeted guiding content, which tends to prescribe particular consumer behaviour and therefore to exclude particular actors form the subject assemblage.

Yet another resistance strategy is to use tools which monitor the flow of information through the boundary object such as Data selfie. This technology also does not protect the user from objectification. Nevertheless it provides visualization of the information provided to traders and thus helps to enact reflexive objectification. To put it simply, the user cannot escape being turned into object, but she can at least partially control the shape of the object she is being turned into.

## b. Overseers

Other important intruders into the personal informational privacy are the overseers, most frequently the state. Through various practices and tools the state controls numerous aspects of our tracks that we daily leave in the infosphere. Most vividly this was revealed during the Snowden controversy in 2013. Edward Snowden is a former employee of the Booz Allen Hamilton (BAH) consultancy company, which was a subcontractor providing electronical surveillance for the National Security Agency (NSA). Back in 2013 Edward Snowden leaked classified information revealing the surveillance practices to which the American and non-American citizens are subjected mainly via their digital and phone communication (Greenwald 2013).

The state surveillance focuses on individuals because individual is the true object of the state (Foucault 2000, 414). The goal of the informational agencies is to create a large database based on which it would be able to reconstruct the behaviour of particular persons. On the first look it may not seem so drastic, because western societies are already accustomed to self-discipline (Foucault 1995, 201). However according to John Doe if we control the data that we produce and provide to the infosphere, does not mean that we can control how the information agencies interpret and what they make of those data.

The experiment of American sociologist Janet Vertesi can serve as an example of such object-manipulations in the infosphere. In reaction to the *Target case* Vertesi tried in 2014 to opt out form the infosphere and hide her pregnancy from the data brokers and other corporate

actors. Vertesi thus avoided for nine months any activity online that could result in disclosure of her maternity. She asked her friends and family not to congratulate her on social media and she visited baby related websites, only through Tor browser, an anonymized web browser using chain of multiple IP addresses in order to make the tracking of users more difficult. Vertesi also had to adjust her shopping habits:

> [W]hen it came to shopping, I did all my purchasing—from prenatal vitamins to baby gear and maternity wear—in cash. No matter how good the deal, I turned down loyalty-card swipes. I even set up an Amazon.com account tied to an email address hosted on a personal server, delivering to a locker, and paid with gift cards purchased with cash. (Vertesi 2014)

As a result of these practices Vertesi was labelled as a criminal by the authorities. Even though Vertesi very cautiously controlled the information provided by her to the infosphere, the interpretation made by the surveillance systems were totally beyond her reach and she was classified as a threat because her overly secretive behaviour indicated illicit activities.

If we interpret Vertesi's case through the prism of reality enactment we can see how tracking devices are exhausting the actors they interact with only to a certain level and thus they create completely new objects. What was for Vertesi in her interaction with colleagues and family members interesting (even though sometimes quite annoying) experiment, was in her interaction with the infosphere highly suspicious behaviour.

Consequently overseers in the infosphere create the disciplined subject as described by Foucault in *Discipline and punish* (1995). Sherry Turkle's (2012) informer Julia shows how just an idea of overseers' presence in the infosphere disciplines teenagers:

> [Julia] and her friends believe that school officials and the police look at students' MySpace accounts. Julia's response is to police herself and watch over her friends. "I'm, like, always telling them, 'Don't put that picture up there. You'll get into trouble.'" (Turkle 2012, 253)

This highly reminds the practice of Amazonian Runa, as described by Kohn. The belief in Runa is that if I don't lie on my back, I won't get turned into prey, an object. In the infosphere the belief is that if I don't do anything suspicious I won't get turned into a suspect, also an object. In each hyperobject the subjects have to resist constant attacks on their subjectivity; they have to negotiate it with other actors. In panopticon this is the program of action; the desirable outcome of the techno-social setting.

That is mainly because Foucault's genius lays not only in his brilliant analysis, opening the black-boxes of what we call human subject; but also in his influential power to repeatedly bring the reality he describes into being. In other words Foucault with his *panopticism* became inseparable part of the reality it described. Turkle provides us with great example of such enactment:

> At a pre-awards cocktail party, one Web luminary spoke to me with animation about the wiretapping controversy. To my surprise, he cited Michel Foucault on the panopticon to explain why he was not worried about privacy on the Internet. […] By analogy, said my Webby conversation partner, on the Internet, someone might always be watching, so it doesn't matter if, from time to time, someone actually is. As long as you are not doing anything wrong, you are safe. Foucault's critical take on disciplinary society had, in the

> hands of this technology guru, become a justification for the U.S. government to use the Internet to spy on its citizens. All around us at the cocktail party, there were nods of assent. (Turkle 2012, 262-263)

In Turkle's example we can see how various actors merge together and how social theory is being enacted through new technologies, institutions and individuals in innovative way. Foucault's analysis is in this case being stabilized and turned from criticism, hence the *matter of concern,* into justified *matter of fact*.

### i. Metadata as objectifiers

As means of control in Vertesi's case served mainly so called *metadata*. First who famously alerted the public about the abuse of meta-data from government was already mentioned Snowden. Meta-data are basically side products of our activities in infosphere; geolocation of our smartphones, histories of our transaction made by credit cards, times of users log-ins, duration of her phone calls or receivers of her e-mails. Basically it is the data about the data we produce in interaction with *traders* and other users. John Doe despite his support of collecting data from traders also admits that there is a problem when data collected separately by traders can be put and analysed together.

Glenn Greenwald, the journalist whom Snowden directly handed and explained the classified materials, describes the nature of and possibilities resulting from the court order aimed against Verizon, one of the largest telephone companies in US, to store and hand over the metadata to NSA:

> While the order itself does not include either the contents of messages or the personal information of the subscriber of any particular cell number, its collection would allow the NSA to build easily a comprehensive picture of who any individual contacted, how and when, and possibly from where, retrospectively. (Greenwald 2013)

Nevertheless the state is not the only overseer. The overseer could be also the employer, or any other actor aiming on creating a picture of individual's behaviour in the infosphere in order to control her. Great example of an employer using ICTs with the intention of controlling users provides Karen C. Levy (2015) in her study about the US truckers using the electronic on-board recorder (EOBR).

The EOBR is a tracking device, which is being implemented mainly by big trucking companies and thus is affecting mostly truckers who work as employees. The employer than can collect various sorts of data from multiple truckers and compare them together. Such data include mainly position of the trucker and activity in which the trucker currently engages, i.e. driving, loading or having a break. The system is employed to replace older paper logs, where the truckers used to fill reports about their work performance.

The problem with EOBR is – according to Levy – that the drivers feel reduced to mere mindless robots. Because the dispatcher can confront their claims (based on their embodied experience) about their current state and situation on the road with other sources such as weather forecast or movement of other trucks, the ability of the truckers for autonomous decision making is drastically lessened (Levy 2015, 169). This illustrates how overseer's surveillance practices completely change the reality of the overseen. The cyborg consisting of

the driver and EOBR is way less autonomous than the cyborg of a driver only with his a car and his road map.

### ii. Bitcoin as libertarian subjectifier

Thanks to the centralization of the internet in the 21st century it is very difficult to avoid the intrusion into privacy from overseers. That is mainly because states and other overseers are usually providers of or can in accordance with their legislation influence ICTs' infrastructures. Erdogan's Turkey and its ban on Wikipedia offer us most current example of this power (Sezer & Dolan 2017). One of the effective legal ways to avoid states power over the informational infrastructures is to use parallel infrastructures which are independent on state by design. One such infrastructure is decentralized technology called *blockchain* which is used mainly to operate various cryptocurrencies such as Bitcoin or Monero.

When in 2011 the US government prohibited banking institutions such as MasterCard or PayPal to provide financial services to the hacktivist web WikiLeaks run by Julian Assange – to protect the cash flow from various supporters – WikiLeaks started accepting cryptocurrencies, namely Bitcoin. This is one of the most known examples of legal resistance towards the overseer's regulation.

Bitcoin is a cryptocurrency developed in 2008 by Satoshi Nakamoto, a fictional person whose true identity remains unknown till this day. Bitcoin uses a decentralized network of computers, so-called *Blockchain*, which connects several thousand devices providing decentralized database of transactional history of each digital token. Keeping this track of transactional history prevents the tokens from double spending.

Each actor participating in releasing new Bitcoins into circulation – Bitcoin miner – lends his computational capacity to the network so the ongoing transactions can be verified. Thus each miner downloads to his computer the whole history of every Bitcoin transaction in a block-chain file. New bitcoin is then released as reward for miners, every time a new block of transactions is verified and can be added to the blockchain of previous transactions.

The main goal of Bitcoin is not to secure anonymity of the users – that is why Bitcoin is not called anonymous, but rather pseudonymous currency. Bitcoin is instead designed to make the physical body of its owner and the token inseparable. Bitcoin thus uses the features of infosphere, namely its non-locality, to individualize the actors in innovative way. John Doe described this inseparability on the case of Ross Ulbricht, the former operator of one of the biggest darknet market places called *Silk Road*.

When Ulbricht was in 2015 sentenced by US court for money laundering, gun and drugs trafficking and other illegal activities which took place on Silk Road, the Us government was not able to confiscate his assets in bitcoins. That is because bitcoin eliminates third parties from monetary transaction such as banks or states. There is thus no actor – except for Ulbricht himself – who would hand over Ulbricht's assets to the government. The tokens are secured by a code which knows only Ulbricht an their history of owners is inscribed into decentralized network, so even if government (or any other party) would try to rewrite the records in one document, there still would be thousands of other copies proving this action invalid.

Some people I've met during the Hackers congress (HCPP 2016) were even using RFID (Radio-frequency identification) implants in their hands in order to store the encryption keys enabling them to use their bitcoin wallets. Dutch entrepreneur Martijn Wismeijer, one of the

speakers on the HCPP, has even two such implants (one in each hand) and he describes this merger of his body with technology as turning his body into an *offshore*.[17] Bitcoin thus in order to overcome the power of state over one's assets co-constructs a libertarian subject.

As Foucault claims, neoliberal state controls its citizens through turning them in responsible neoliberal subjects. Being a neoliberal subject means that very individual is basically a little enterprise herself (Foucault 2011, 175; 225). This means that every choice an individual makes are little investments into his human capital increasing or decreasing value of his assets. The libertarian subject goes even further with this logic and declares individual an offshore; a unit economically independent on state regulation. Here comes handy the analysis of global assemblages by Saskia Sassen (2006) for it is those assemblages, what co-shapes the quasi-subject. Sassen argues that features of a "previous" phase evince the feature of a current phase (2006, 16). In this case it would be feature of neoliberal subject with its accent on individualization and responsibilization but within the realm of state, which gave rise to the libertarian subject rejecting the regulatory power of the state establishing alternative technologically mediated community.

Thus the aim of Bitcoin inscribed in its design, is to protect the libertarian subject from various state interventions; whether it be central interventions into the economy or repossession of the subject's assets. On this count Bitcoin is a privacy maintaining technology, for it creates a subject inseparable from its means of exchange and helps her to win the struggle over control of these means. It does not resist the individualization practices of the overseer; it rather uses them for different purpose and therefore creating new possibilities for resistance.

Another cryptocurrency using blockchain is *Monero*. Monero works on similar principles as Bitcoin but it adds one key element to the assemblage, and that is anonymity. Monero in order to protect the identity of people entering into monetary transactions uses basically the same principle described in the John Doe cases. It creates shared identity of the subject entering the transactions by separating the amount of cash they are sending into various smaller amounts and then again collecting these smaller amounts into the desired sum at the side of the receiver. The trick is that the receivers sum is collected from various senders, thus it is impossible to identify an individual; overseers can only identify the group of three or (ideally) more senders.

The developers and users of the Monero thus very well understand the individualizing tendencies of the overseers and they resist them by implementing a shared identity into the very design of the currency. If the individualization is the program of the overseers' surveillance tools, the shared identity is an anti-program implemented into parallel technology. The aim is to create dispersed unidentifiable subjectivities which cannot be turned into individualized objects.[18]

[17] Talk given during the HCPP2016 on 2.10.2016. Wismeijer talks about this topic also in an interview for Liberty Entrepreneurs available online: https://www.youtube.com/watch?v=8sQV3rT6pLU (retriever 9.5.2017)

[18] It is often argued that such cryptocurrencies support illegal economy such as drug trafficking, child pornography etc. Nevertheless John Doe argues that most of the transactions in global illegal economy are still executed in US dollars.

### iii. Summary

The overseers' goal is to turn users into individualized objects which are directly identifiable and whose bodies and deeds in the infosphere form inseparable unity. The overseers work in this way, because individuals are the main objects of their power, and it is in overseers' interest to police individuals. The overseers create individualized objects by collecting data about users' communication in the infosphere whether it be communication between users, or communication between users and traders.

There are just a few strategies how to resist overseer's power over individual in the infosphere. One is to go along and discipline itself; that is the program of action in modern panopticon. Bu that also can mean that one has to accept the program of action of traders, because otherwise her behavior would result into investigation.

The other mode of resistance is to use parallel infrastructures, which enable different kinds of individual or collective assemblages. These infrastructures and technologies allow to partially eliminate the presence of overseers from the subject assemblage.

## c. Criminals

In the spring of 2017 Czech president Miloš Zeman accused unknown hackers of installing child pornography into his computer later claiming that the traces of the hackers lead to Alabama in US. When I discussed this case with John Doe, he laughed and explained why this is highly implausible:

> Everybody who is engaged with hacking knows what not to do. You never attack someone from your own computer directly; you use other computers in the network to do the dirty work for you. You install bots into those computers and create a chain of them so it gets difficult, nearly impossible to track you back. This is also the reason why it is stupid and dangerous to connect to the network directly without using a firewall or some kind of anti-virus, because then you risk that your computer will be seized by some third party and used for an unknown purpose. (John Doe, April 2017)

The basic aim of the criminals in the infosphere is to gain access to data and manipulate those data beyond owner's control. The data can be copied, deleted or even locked and held hostage. The attacked data don't have to belong only to individuals, but can also be property of states, corporations or even multiple owners; for example personal passwords show how the ownership of data can be shared, for those passwords can be stolen not only form individuals computers, but also from companies' databases.

Criminals are in the infosphere a wild card, they are deviants and their action can be considered intrusion into privacy or it can be interpreted as from of resistance towards other actors. For example *Wikileaks* or *Anonymous* are considered criminals by state authorities, but on the other hand they can also lessen the informational asymmetry in the infosphere through so-called counter-veilance. Important is, that criminals always enact a form of antiprogram. As such they move outside, destabilize and challenge ontological categories of self and non-self, human and non-human.

At this point I am certainly not advocating criminal activities in the infosphere. But their practices – especially the successful ones – may serve as critical signifiers uncovering the naturalized design of infosphere in the future.

### i. Malware and non/self-recognition

Malware is a shortcut for malicious software and the most common label for malware is "computer virus". The first computer (proto-)virus appeared already in 1971 running on TENEX operational program, spreading through the Arpanet (first version of internet). Name of the software was Creeper and at the same time was written also its nemesis Reaper; basically the first anti-virus (Szor 2005, 41). Creeper was simply copying itself through the ARPA network and showing a short message on every computer, to which it gained access, reading: "I'm the Creeper, catch me if you can!" (Metcalf 2014) Reaper was designed to search for creeper and delete it.

Ever since then more and more sophisticated programmes with aims of self-replication and uncontrolled spread through the network are being created. The motivations behind their spread may vary from fun of reckless teenagers to theft of data to attack on the users – i.e. by downloading incriminating materials such as child pornography into her computer[19].

The most used means against criminals and their intrusion into privacy is usually antivirus software to which is delegated the recognition of self from non-self. The function of the antivirus is to recognize suspicious behaviour inside the computer behind the user interface. If the antivirus identifies some parts of the software behaving in unstandardized manners, it identifies the part of the software as malware, informs the user and blocks the malware from operating.

In dealing with malware and criminals generally the recognition of desirable from undesirable – whether it's human from non-human, or self-from non-self – actors in the interaction is very important. John Doe while describing me how he was extracting the data from LinkedIn provided me with nice example. Even though he wasn't breaking the law, he was violating the rules of use by using a data-scraping bot. Such bot is a piece of software which enters the network in disguise for human user and extracts the data form public profiles.

> I ended up scraping LinkedIn actually and I was with a programmer who created a scraper and after while LinkedIn was like: "Ok. This is no human exploring our website." So we get out of it and we had to make this scraping process a bit more *humanlike*. (John Doe, January 2017)

The LinkedIn algorithms discovered the bot because they identified its behaviour as "not enough human". LinkedIn thanks to its own databases capturing the human behaviour on their network can create a model of standardized human user; once any user does not fit such standardized model, she is banned.

Same thing is done by antivirus and other security software when it identifies that some program in the computer is behaving in non-standardized manner. Such recognition is for humans almost impossible because lots of non-human interaction in a computer is going behind the interface and is completely invisible to the human user. All these actors work basically as sieve: "a mechanical devices separating desired materials from undesired materials." (Kockelman 2013, 35) But the sieve as mediator – similarly as Mongolian

[19] Few years back this kind of attack was also offered on one of the darknet market places for several thousand dollars depending on the security of target. Part of this "service" was also reporting the presence of illegal content to the authorities in order to cause criminal prosecution of the victim.

shamanic gown – exhibit kind of intimacy with the substances they are sieving (Kockelman 2013, 35). Thus sieving out undesired actors still creates form of connection with them; that means that even those which are sieved out partially enter the quasi-subject and both are mutually shaped by each other. The undesirable is trying to mimic the features of the sieve and the sieve has to react.

Anthropologist Mathew Bernius provides another good example when he describes his encounter with a non-human actor on the internet. Bernius was looking for informers in chatrooms for his research concerning webcam users. That's where he met AZ_Tifanny:

> I private-messengered (PM'd) Tiffany and, after a bit of negotiation, offered to join her website in exchange for an interview. She agreed and I left to sign up. After paying the one-day membership fee, I discovered that the site was a façade. […] Back in the chatroom, I PM'd her for an explanation […] but [she] did not address my questions. […] All at once the embarrassing truth of the situation dawned on me. A quick scan of our archived conversation confirmed my suspicion: Az_Tiffany was not a cam girl; she wasn't even a person. Az_Tiffany was a chatbot. […] I had been [tricked] by a machine. (Bernius 2012, 54)

In this example Bernius shows how the non-human – undesirable entity in chatrooms – mimicked his sieve (partially deformed by his enthusiast expectation of an informer [2012, 58]) and tricked him into perceiving Tiffany as a desirable entity. Only after a disappointment and recalibration of his sieve Bernius was able to uncover how Tifanny mislead him.

Bernius also further describes what happens to chatbots like Tifanny when they get discovered. Usually their authors take them and try to rewrite their script so it would appear more humanlike than before, they identify the mistake which gave away the chatbot and try to avoid them. (Bernius 2012, 55-56)

Malware does the same while trying to avoid the sieve of anti-virus and anti-virus always has to react quickly to new shapes the malware takes. That is why most antivirus software perform better while they are connected to the web, because they can share new forms of viruses in order to avoid them. By analogy we can say that they learn from each other through the infosphere.

The same happens to humans, they also have to learn from each other in order to protect their devices. Nowadays it is considered highly irresponsible to open an e-mail from a friend reading: "Hey pal, check this out!" with attached link, because such a general message is probably produced by a malware occupying friend's computer, which is trying to mimic human interaction. At the same time it is basically plain stupid to write such an email with overly general text and attached link, which I did few months back. The immediate response from a friend, whom I send such an email, was: "What's this? Is it a malware?" On this simple example I try to illustrate how in the environment where predation through mimics occurs on daily basis people have to constantly renegotiate signs signifying their human status in their interaction.

### ii. Summary

While in the previous cases in the overseers and traders it is mainly negotiated what it means to be subject or object in terms of power, criminals and malware contest such ontological negotiations also inn terms of equal interaction. In other words one has to prove his

subjectivity through various subjectifiers not only to himself (i.e. through sieving undesirable actors from the quasi-subject assemblage) but also to others (i.e. through not sending overly general messages).

The presence of criminals in the infosphere shows us how the naturalized categories of humans and non-humans are also challenged and that their enactment depends on the hyperobject which mediates them. Different technologies and techniques are used to enact the human/non-human distinction between the Runa and their dogs, and between a human user and malware in the email inbox.

## 6. Ontological politics through design

From the few examples mentioned above we can see that the actors are being translated by the hyperobject of infosphere. The list of the ways they are translated is definitely far from being exhaustive; there is basically endless variety of how the quasi-subject/object can be assembled in particular encounters. What is my point here is rather that this assembling is always an open-ended process (Latour 2007, 217; Floridi 2014, 60-61). Such process also results into the multiplicity of cyborgs created in the process of becoming, best visible on the Vertessi case. Her status of quasi-subject resisting the objectification from traders was basically contradictory with her status of quasi-object assembled by the overseer.

Overseers and Traders are using the boundary objects in the infosphere as a one way mirror, except now the mirror is not a hole in a wall at the police station or marketing research agency, but is on our desks and in our pockets. "The screen is a monitor and is monitoring you." (Floridi 2005, 192) It is Bentham's Panopticon made more durable through technology. Whereas the Panopticon was aiming to create through technology closed and controllable environment, current ICTs are reversing this process and change the environment outside of them in order to make it more predictable (Floridi 2014, 97-98).

Therefore there is no *away* anymore, where the problems generated by these technologies could be sent to. Similarly as with the dust in Bangkok which cannot be sent away and could be rather cumulated on the *Dusty relief*, we have to learn how to deal with certain problems generated by the infosphere. We cannot send particular actors away because there is no away, the state, corporations and criminals will still be in this space, but we have to learn how to channel and deal with them to lessen the power asymmetry. John Doe supports this argument with his claim:

> To say that global surveillance is not good and prohibit it by i.e. democratic process and say now we have solved it, that is not a solution. Once there is this possibility to control, it will be used. (John Doe, April 2017)

The infosphere offers lots of tools and strategies which can help us to be more reflexive, yet these tools have to be maintained and constantly improved or else the intruders always find a new way how to overcome them and make them obsolete. For John Doe thus the privacy protection shall be implied in digital platforms "by default". That also means not laying all responsibility on the "end user" of boundary objects. "If informational privacy is conceptualized purely as individual choice it misses out on a great number of significant moves in contemporary society that go beyond the individual's ability to make conscious

decisions about their own informational-self." (Mai 2016, 196) The ability to make informed decisions concerning our personal data thus has to be inscribed in the technology, if we want to lessen the power asymmetries in the infosphere.

This poses big ethical questions concerning technology and design of the infosphere. The intrusions of personal space in infosphere are morally questionable from different ethical perspectives at the same time. For one member of German artist/activist group, called *Peng Collective,* invasion of privacy is wrong not only because our personal information can be abused by the intruder (thus from *consequentialist* perspective) but it is basically morally wrong in itself (therefore also from the perspective of *deontology*).[20]

The consequentialist perspective is according to Floridi not sufficient because unauthorized gathering and the misuse of private information can be justified, especially when *common good* or *public interest* come into play (2005, 193). Consequentialist perspective then does not allow any stable point of reference, because each actor in the assemblage can argue from different positions with different goals. Therefore the best consequences justifying the intrusion of privacy form overseers may be the *safety of citizens* and from traders the *improvement of customer experience.*

My argument is that in order to establish more equal access to means of self-production and control we should employ mainly Kant's deontology principles. Given that Kant's first categorical imperative reads: "Act only in accordance with that maxim through which you can at the same time will that it become a universal law," (Kant 2002 [1785], 37) it can be concluded that this ethical approach is basically ontological politics. That is for it says that we shall always act with the idea, that reality is enacted by our actions. That does not concern only human actors, but also non-humans. By that I am not proposing that non-human actors shall be held morally responsible for the enactments on which they participate, but their ability to shape reality bears ethical dimension which should be reflected in their design. In other words, while designing our technologies we always should ask which kind of reality we want them to enact, or rather enable for enactment.

Second Kant's categorical imperative reads: "Act so that you use humanity, as much in your own person as in the person of every other, always at the same time as end and never merely as means." (Kant 2002 [1785], 46-47) This formulation is then in direct contradiction with practices of privacy intruders. Violation of this ethical rule is basically inscribed in the centralized nature of the infosphere, where there are few obligatory passage points through which various actors can harvest personal information. These passage points are mainly providers of virtual services such as Google or Facebook and also the operators of the informational infrastructure. Providers of services use the data themselves for profits whereas the operators are regulated by national governments to provide metadata as means of control. To treat humanity as an end would mean to restore symmetry to the process of data collecting and especially processing. Decentralized digital platforms as blockchain show us that such setting is possible, although John Doe alongside many other propagators of Bitcoin or Monero are afraid that these technologies will be criminalized in the future.

If we apply the first imperative to traders and overseers so their practice shall become a universal law, it would necessarily mean that even their own data would be "open for

[20] Talk given 1.10.2016 during HCPP 2016 called *Intel exit.*

business". The beauty of Kant is in his avoidance of consequences, using them merely as illustrations but never as arguments. Kant's ethics creates logical paradoxes instead.[21] In a reality where it is acceptable that only a few can enter the privacy of many, privacy seems to disappear. Floridi argues that this is not particularly the case, that privacy in the infosphere is just different (Floridi 2005, 186), but to be made different it has to be enacted as such. And this enactment has to be carried out by multiple actors. The outcome then depends on what modes of action are enabled by/to these actors. To put it simply, the a/symmetry must be designed.

The hyperobject is also as other actors in constant process of becoming and thus it can be changed. But it cannot be changed over-night given the time-space scope it occupies. On the example of Kohn's rainforest we showed that it creates a specific eco-system where actors emerge in mutual interaction, and by changing this eco-system we change ourselves. The question is then who has the power to change the hyperobject? Dominic Boyer and Timothy Morton argue that there used to be a widespread belief that only a *hypersubject* is entitled to change the world: "Hypersubjects are typically, but not exclusively white, male, northern, well-nourished, and modern in all senses of the term." (Boyer & Morton 2016) Hypersubject is the one entitled to the view from nowhere; it is the product and the producer of modernity:

> From the eighteenth to the mid-twentieth centuries, the great historical constructions of gender, race, and class were embedded in the organically marked bodies of woman, the colonized or enslaved, and the worker. Those inhabiting these marked bodies have been symbolically other to the fictive rational self of universal, and so unmarked, species man, a coherent subject. (Haraway 1991d, 210)

In infosphere Steve Jobs, Marc Zuckerberg and Bill Gates are the typical hypersubjects. Not because they would be so extraordinary – they've become mainly synonyms for the companies they founded – but because many people decided to believe in their uniqueness corresponding with the modern myth of *revolutionary inventor* as a coherent subject authorized to inflict his will onto the surrounding world.

But these hypersubjects already inscribed their design into the infosphere – some may even (wrongly) say that they brought the infosphere into being – and the outcome is the asymmetry of *one way mirror* we have to deal with today. Boyer and Morton (2016) thus speak also of *hyposubject* – subject which is multiple, neither one nor many – an anonymous innovator from the margins. Hyposubject does not send things *away;* she lives with the things, recycles them and uses them in innovative ways for her benefit.

According to anthropologist Arjun Appadurai, design is a "fundamental human capacity" (2013, 254) which means that we are all potential designers, but not as hypersubjects, but as hyposubjects. We can all use and maintain designs using the existing properties of infosphere in innovative ways, similarly as it is done by the decentralized blockchain-based technologies. We can support other open-source projects such as Linux or Mozilla, we can use adblocks and

[21] Best example is the current political trend that it is acceptable to lie for a good cause practiced by diverse actors such as PETA or Donald Trump resulting in current wildly discussed crisis of truth (so-called post-truth). For Kant lying is never acceptable for any reason, because the result would be exactly this logical paradox that truth would cease to exist (Kant 2002, 18-19).

data selfies, we can (try to) opt out. “If we wish to thrive, it is as hyposubjects that we will become human (again).” (Boyer & Morton 2016)

This does not mean that everyone shall be responsible for herself; that would be the logic of neoliberalism as described by Foucault. The hyposubject is like a cyborg, she is not innocent (Haraway 1991b, 180). Hyposubject is responsible for the realities she chooses to enact not just for herself, but also for other actors; especially for others. In words of Donna Haraway: “We are responsible for boundaries; *we are they*.” (Ibid., emphasis added)

This weird contradictory character of hyposubject is greatly illustrated on the abovementioned example of block-chain. Despite the libertarian and highly individualistic ideology which is inscribed into the technologies using this platform, the block-chain is based on shared responsibility for its maintenance. Thus in order to be able to act independently each on her own, the hyposubjects must paradoxically work together.

## 7. Conclusion

When nowadays people talk about globally interconnected relations they usually use the term *global village*. Given the information asymmetries inscribed by infosphere I suggest that more accurate would be to call our current situation a *global interrogation room*. That is for in traditional village the access to information through social control is way more symmetrical than is the case in our current condition. In order to establish a village we would need more symmetrical approach to modes of information harvesting and its processing. There should be implemented potentials to better control and reflect on information we share through the infosphere with other actors. One of the possible ways is implementing similar tools as data selfie to multiple platforms so users would be able at least to see the amount and character of information they are paying for using certain services, while gaining a little glimpse how these data are processed and what kind of object is assembled out of them.

In this text I constructed picture of an infosphere as a mediating hyperobject which helps to enact particular kind of reality. I re-constructed informational privacy as a self-constituting practice which is carried out by multiple actors. The text first describes traditional social theories of privacy as a self-making and then develops another post-humanist framework through which such practices can be understood in the information society.

At The starting point of this text I argue that reality in general is open-ended process brought into being by various practices and various actors.

The argument is that in order to become subject in the infosphere, human actors have to be able to control strategical access points to their assemblage called self. This process of control is delegated on or mediated through multiple non-human actors which become subjectifiers, enabling the human actors to regulate their presence in the infosphere.

Without these subjectifiers human actors are being objectified by other actors. Basically there is no escape from the hyperobject and its inscription into bodies, but it is possible to regulate those inscriptions and react to them. Without such regulation one loses the ability to fully control certain dimensions of her self-assemblage and is being turned into an object.

On various cases of traders, overseers and criminals I tried to provide examples of the inscriptions of hyperobject into the self and also different subjectifying strategies which

provide the human actors with ability to resist these inscriptions and channel them in more controllable way.

In the end of the text I propose preferable ethical framing of deontology which best suits to the ontology politics of enactment. Furthermore I Argue that the enactment of more symmetrical reality must abandon the idea of hypersubject – the mythical pure monolithic subject allowed to shape the world of objects – and has to adopt the trope of hyposubject – the subject from the margins equipped with multiple subjectivities as modes of being in the world through negotiation and not domination.

## References:


Ackerman, S. and S. Thielman. (2016) US officially accuses Russia of hacking DNC and interfering with election. *The Guardian*. Online: https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election (Retrieved: 8. 5. 2017)

Appadurai, A. (2013). *The future as cultural fact: essays on the global condition*. Verso Lendon/New York

Barad, K. (2007). *Meeting the universe halfway: Quantum physics and the entanglement of matter and meaning*. duke university Press.

Barrick, M. R., & Mount, M. K. (1991). The big five personality dimensions and job performance: a meta-analysis. *Personnel psychology*, *44*(1), 1-26.

Barthes, R. (1981). *Camera lucida: Reflections on photography*. Macmillan.

Beck, U. (2011). *Riziková společnost: na cestě k jiné moderně* (2. vyd.). Praha: Sociologické nakladatelství.

Bernius, M. (2012). Manufacturing and Encountering 'Human'in the Age of Digital Reproduction. *Human No More: Digital Subjectivities, Unhuman Subjects, and the End of Anthropology*, 49-70.

Blaser, M., Briones, C., Burman, A., Escobar, A., Green, L., Holbraad, M., ... & Blaser, M. (2013). Ontological conflicts and the stories of peoples in spite of Europe: Toward a conversation on political ontology. *Current Anthropology*, *54*(5), 547-568

Boyer, D., & Morton, T. (2016). Hyposubjects. *Theorizing the Contemporary, Cultural Anthropology*.

Butler, O. E. (1987). *Dawn*. New York: Warner.

Chen, T. M., & Robert, J. M. (2004). The evolution of viruses and worms. *Statistical methods in computer security*, *1*.

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso Books.

De Castro, E. V. (1998). Cosmological deixis and Amerindian perspectivism. *Journal of the Royal Anthropological Institute*, 469-488.

Deseriis, M., & Pessoa, F. (2011). Lots of money because I am many': The Luther Blissett project and the multiple-use name strategy. *Cultural Activism: Practices, Dilemmas and Possibilities. Thamyris/Intersecting: Place Sex and Race*, *21*, 65-93.

Douglas, M. (2003). *Purity and danger: An analysis of concepts of pollution and taboo*. Routledge.

Douglas, M. (2004). *Natural symbols: Explorations in cosmology*. Routledge.

Downey, G. L., Dumit, J., & Williams, S. (1995). Cyborg anthropology. *Cultural Anthropology*, *10*(2), 264-269.

Duhigg, C. (2012). How companies learn your secrets. *The New York Times*, *16*, 2012.

Epstein, R. (2016). Empty brain. *Aeon Magazine.* Online: https://aeon.co/essays/your-brain-does-not-process-information-and-it-is-not-a-computer (Retrieved 9.5.2017)

Feyerabend, P. (1993). *Against method*. Verso.

Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology*, *7*(4), 185-200.

Floridi, L. (2014). *The fourth revolution: How the infosphere is reshaping human reality*. OUP Oxford.

Foucault, M. (1995). *Discipline and punish: The birth of the prison*. Vintage.

Foucault, M. (2000). The political technology of individuals. In Foucault, M., & Rabinow, P. (2000). *Power: essential works of Foucault, 1954-1984*. J. D. Faubion (Ed.). New Press.

Foucault, M. (2011). *The birth of biopolitics: Lectures at the college de France, 1978-1979*. New York: Palgrave Macmillan.

Gertz, N. (2016). Autonomy online: Jacques Ellul and the Facebook emotional manipulation study. *Research Ethics*, *12*(1), 55-61.

Gertz, N. (2017) Nihilism - There's an App for That! | Nolen Gertz | TEDxFrankfurt. Available online: https://www.youtube.com/watch?v=GpKrM8GQwOg

Giddens, A. (1990). *The consequences of modernity*. Stanford: Stanford University Press.

Giddens, A. (1991). *Modernity and self-identity: Self and society in the late modern age*. Stanford University Press.

Goffman, E. (1961). *Asylums: essays on the social situation of mental patients and other inmates*. New York: Doubleday.

Graeber, D. (2015). *The utopia of rules: On technology, stupidity, and the secret joys of bureaucracy*. Melville House.

Grassegger, H., & Krogerus, M. (2017). The data that turned the world upside down. Online: https://motherboard.vice.com/en_us/article/how-our-likes-helped-trump-win (Retrieved 17.5.2017)

Greenwald, G. (2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*, *6*(5), 13.

Haraway, D. J. (1991). *Simians, cyborgs, and women: The reinvention of nature*. Routledge/New York.

Haraway, D. J. (1991a) The biological enterprise: Sex, mind, and profit from human engineering to sociobiology. in Haraway, D. J. *Simians, Cyborgs and women: The reinvention of nature*, 43-68.

Haraway, D. J. (1991b). Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieeth Century. in Haraway, D. J. *Simians, Cyborgs and women: The reinvention of nature*, 149-181.

Haraway, D. J. (1991c). Situated knowledges: The science question in feminism and the privilege of partial perspective. In Haraway, D. J. *Simians, Cyborgs and women: The reinvention of nature*, 183-201.

Haraway, D. J. (1991d). The biopolitics of postmodern bodies: Determinations of self in immune system discourse. In Haraway, D. J. *Simians, Cyborgs and women: The reinvention of nature*, 203-230.

Haraway, D. J. (1997). *Modest_ Witness@ Second_Millennium. FemaleMan©_ Meets_OncoMouse™: Feminism and Technoscience*. Psychology Press.

Haraway, D. J. (2008). *When species meet.* University of Minnesota Press.

Harman, G. (2009). *Prince of networks: Bruno Latour and metaphysics*. Prahran, Vic.: Re. press, 2009..

Hayles, N. K. (1993). The materiality of informatics. *Configurations*, *1*(1), 147-170.

Hayles, N. K. (2008). *How we became posthuman: Virtual bodies in cybernetics, literature, and informatics*. University of Chicago Press.

Heidegger, M. (1977). *The question concerning technology, and other essays*. New York: Harper & Row.

Helmreich, S. (1998). *Silicon Second Nature: Culturing Artificial Life in a Digital World, Updated With a New Preface*. Univ of California Press.

Kant, I. (2002) *Groundwork for the metaphysics of morals*. New Haven: Yale University Press

Kohn, E. (2013). *How forests think: Toward an anthropology beyond the human*. Univ of California Press.

Kuhn, T. S. (1975). *The Structure of Scientific Revolutions: 2d Ed., enl*. University of Chicago Press.

Kurzweil, R. (2005). *The singularity is near: When humans transcend biology*. Penguin.

Kurzweil, R. (2012). *How to create a mind: The secret of human thought revealed*. Penguin.

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Harvard university press.

Latour, B. (1990). Technology is society made durable. *The Sociological Review*, *38*(S1), 103-131.

Latour, B. (1994). On technical mediation. *Common knowledge*, *3*(2), 29-64.

Latour, B. (2007). *Reassembling the social*. Hampshire: Oxford University Press, 2007

Law, J. (2004). *After method: Mess in social science research*. Routledge.

Law, J., & Urry, J. (2004). Enacting the social. *Economy and society*, *33*(3), 390-410.

Lupton, D. (2014). Self-tracking cultures: towards a sociology of personal informatics. In *Proceedings of the 26th Australian Computer-Human Interaction Conference on Designing Futures: the Future of Design* (pp. 77-86). ACM.

Lupton, D. (2016). Digital companion species and eating data: Implications for theorising digital data–human assemblages. *Big Data & Society*, *3*(1).

Mai, J. E. (2016). Big data privacy: The datafication of personal information. *The Information Society*, *32*(3), 192-199.

Marx, K., & Engels, F. (2002). *The communist manifesto*. Penguin.

McCray, W. Patrick. (2016) "It's Not All Lightbulbs". *Aeon Magazine*. Online: https://aeon.co/essays/most-of-the-time-innovators-don-t-move-fast-and-break-things (Retrieved 9.5.2017)

Metcalf, J. (2014). *"Core War: Creeper & Reaper"* online: http://corewar.co.uk/creeper.htm (Retrieved 7.5.2017)

Mol, A. (1999). Ontological politics. A word and some questions. *The Sociological Review*, *47*(S1), 74-89.

Mollen, J. (2015). Pirate Bay Founder:"I Have Given Up." *Motherboard*. Online: https://motherboard.vice.com/en_us/article/pirate-bay-founder-peter-sunde-i-have-given-up?utm_source=dmfb (Retrieved: 7.5.2017)

Moore, M. (2009). Gay men'can be identified by their Facebook friends'. *The Telegraph*, *21*. Online: http://www.telegraph.co.uk/technology/facebook/6213590/Gay-men-can-be-identified-by-their-Facebook-friends.html (Retrieved 7.5.2017)

Moravec, H. (1988). *Mind children: The future of robot and human intelligence*. Harvard University Press.

Morton T. (2013). *Hyperobjects: Philosophy and Ecology After the End of the World.* Minneapolis: University of Minnesota Press

Morton, T. (2016). *Dark Ecology: For a Logic of Future Coexistence*. Columbia University Press.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Okely, J. (1983). *The traveller-gypsies*. Cambridge University Press.

Pedersen, M. A. (2011). *Not quite shamans: spirit worlds and political lives in northern Mongolia*. Cornell University Press.

Pedersen, M. A. (2014). The fetish of connectivity. in Harvey, Penny, et al. (Eds.) *Objects and materials: A Routledge companion*. Routledge, 2014.

Popescu, M., & Baruh, L. (2013). Captive but mobile: Privacy concerns and remedies for the mobile environment. *The Information Society*, *29*(5), 272-286.

Rey, P. J., & Boesel, W. E. (2014). The Web, digital prostheses, and augmented subjectivity. in Kleinman, D. L., & Moore (Eds.), *Routledge handbook of science, technology, and society.*– NY: Routledge, 173-188.

Roberts, L. (2016). Personal communication

Rousseau, J. J., (2002). *The social contract: And, the first and second discourses*. Yale University Press.

Sassen, S. (2006). *Territory, authority, rights: From medieval to global assemblages* (Vol. 4). Princeton, NJ: Princeton university press.

Schwartz, B. (1968). The social psychology of privacy. *American Journal of Sociology*, *73*(6), 741-752.

Sezer, C. & Dolan D. (2017) Turkey blocks access to Wikipedia. *Reuters*. Online: http://www.reuters.com/article/us-turkey-security-internet-wikipedia-idUSKBN17V06Q (Retrieved: 18.5.2017)

Stanley, J. and B. Wizner (2013) Why the government wants your metadata. *Reuters,* online: http://www.reuters.com/article/idUS405151053420130607 (Retrieved 7.5.2017)

Star, S. L. (1990). Power, technology and the phenomenology of conventions: on being allergic to onions. *The Sociological Review*, *38*(S1), 26-56.

Star, S. L., & Griesemer, J. R. (1989). Institutional ecology, 'translations' and boundary objects: Amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39. *Social studies of science*, *19*(3), 387-420.

*The Economist* (2017) Fuel of the future: Data is giving rise to a new economy. Published 6th May, 2017, online: http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy (Retrieved: 14.5.2017)

Turkle, S. (2012). *Alone together: Why we expect more from technology and less from each other*. Basic books.

Verbeek, P. P. (2010). *What things do: Philosophical reflections on technology, agency, and design*. Penn State Press.

Verdery, K. (1996). *What was socialism, and what comes next?* Princeton: Princeton University Press.

Verdery, K. (2014). Ethnography in the Securitate Archive. *Acta Universitatis Sapientiae. Social Analysis*, *4*(1/2), 7.

Vertesi, J. (2014). My experiment opting out of big data made me look like a criminal. *Time, May*, *1*.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard law review*, 193-220.

Weber, M. (2001). *The Protestant ethic and the" spirit" of capitalism and other writings*. Routledge Classics.

White, L. (2013). Energy and tools. In Erickson, P. A., & Murphy, L. D. (Eds.). *Readings for a history of anthropological theory*. University of Toronto Press.

Wyatt, E. (2013). A Victory for Google as FTC Takes No Formal Steps. *New York Times, édition du*, *4*.

## Attachments:

Figure 1: Me and John Doe – February 2017