Dominik Stosik[1]

#DeathToFreedomOfSpeech

Abstract

In this analysis the author sets out to examine the concept of freedom of speech on the internet, drawing upon the development of the World Wide Web, the Big-Data-Trade-Off-Dilemma and the nothing-to-hide argument fallacy. A key finding is the observation of a multitude of emerging challenges in the field of ethics, privacy, law and security. Furthermore the most recent exertion of influence on the freedom of speech, that is to say astroturfing should adduce as an instance to demonstrate the possibilities of manipulating public opinion. Further on, the analysis of governmental military enhancement programmes and the example of a recent entertainment programme production shall serve as a visualisation that the research on unprecedented signal resolution and data-transfer bandwidth between the brain and electronics might be far more close to reality than one might be expecting. The results suggest that the freedom of speech is preceded by the freedom of thinking. Its manipulation on a bigger scale (e.g. national elections) could serve as a new way of psychological warfare and therefore the freedom of thinking, or the right to a free mind should remain unviolated.

Key words: privacy, bioethics, neuroethics

"Laws and ethics can't keep pace with technology" (Wadhwa, 2014). The internet, originally conceived in the 1960s and developed in the 1980s as a scientific network for exchanging information, was not designed for the purpose of separating information flows (Michener, 1999). The Word Wide Web as we know it was not foreseen, neither was the evolution of ways in how we access it. Developments over recent years have each created new ethical and legal challenges, e.g. the discussion around the use of cookies (Palmer, 2005), the "like" button (Krishnamurthy & Wills, 2009), cloud

[1] MA; Wrocław Medical University; e-mail: dominik.stosik@student.umed.wroc.pl.

computing (Ruiter & Warnier, 2011), and the interactive web, known as Web 2.0, where users generate much of the content themselves.

In increasing numbers, devices other than smartphones, such as watches, refrigerators and cars, that are not limited to user-owned computing devices, will be connected to the internet, containing chips and/or connected in the so-called Internet of Things.

DeNardis (2014) notes that individuals using a social media platform or smartphone app may have the impression that their online activities are private, but in practice, much more information is collected, some of which is not related to content but to associated information to identify the user in an administrative and logistical way. Some services collect information as device information, including unique hardware identifiers, mobile phone number (if accessing the internet from a phone), IP address, time and date of phone calls, actual location based on GPS, Wi-Fi, or cellular signal from a mobile device. Above all, it seems pertinent to remember that some of this information might not necessarily be needed to provide a particular service. Following the line of argument by DeNardis, the gathering and sharing of data about individuals is at the heart of both online advertising and new forms of government surveillance or, to put it another way, we are facing a situation that Gallagher (2014, p. 5) calls "multiveillance", which is surveillance not just by the state but also by companies, marketers, and those in our social networks.

The most compelling argument within the Big Data discourse is that the user has become the product and is not the customer any more. Although those who are involved in the "free software movement" advocate for "free" as in free speech (Latin: *libre*) rather than "free" as in free beer (Latin: *gratis*), what has occurred in practice, and is still taking place, is a supremacy of software as free as in free beer. The public does not feel that they are paying for the use of social media platforms: Facebook or Twitter, or internet search engines such as Google, Yahoo!, or Bing. Provided that maintaining those services costs a lot of money and provided that anything can become something of value, one could conclude that not only has personal data become the currency the user is paying those services with, but also "the world's most valuable resource is no longer oil, but data" (Regulating, 2017), the fuel of the future.

We see that there is a transformation from *ad valorem* to *gratis* software, which still is an ongoing process and which makes it difficult to draw definite conclusions. With this in mind, let us look at the possible

motivations that make people put themselves in an exposed position on the internet. In order to understand these motivations, which may only be limited to assumptions, we need first to understand which information people think is available about themselves online. In light of the evidence from a survey entitled *Anonymity, Privacy, and Security Online* (Rainie, Kiesler, Kang & Madden, 2013), we have a better understanding of what adult internet users say which information about them is available online. Thus, 66% of them think it is "a photo of you", 50% think it is their birth date, followed by general information such as home address, phone number and the company one works for.

If things were only that simple. Consider for a moment the records that Google has of your searches you did on the internet: records of your wonderings, musings, and fantasies. Think of the records your e-mail provider has of your communications, or a cloud company has of your documents. Consider the (machine learning) algorithms behind all those services that make them improve with every input by every internet user.

Although the possibilities of the internet to keep in touch with one another are very convenient, think for a moment about the records social networks hold concerning their users. Possible motivations in addition to usefulness could be derived from an evolutionary point of view. Human beings are by nature social animals. In other words, it may appear convenient to have all of your contacts within shouting distance, that is, not too far away, but also not too close. Psychologically speaking, one could assume that some people might fear that they will not exist if they do not have an online identity, since studies (Ong et al., 2011) suggest a link between narcissism, extraversion and adolescents' self-presentation on social media platforms. Furthermore, there is evidence to support this theory considering the ingenious methods how social media platforms remind their users on a constant basis to "complete" their profiles, which basically is nothing more than adding more personal information.

Another key point to remember is that social media services tend towards the creation of an allegedly wholesome shell of positivity, where users get to express themselves by liking something and others receiving those likes, which is a manufactured mutual win-win situation by default, considering that there was and is no "dislike" button. Recently, Facebook users got upgraded from expressing one emotion up to 6 basic emotions, in addition to the "like" button there now is "love", "haha", "wow", "sad" and "angry". Similar to the limitation of expression in order to keep the

atmosphere positive, the idea of an ideal online world is kept alive by, for example, only notifying users that they have gained a new friend, but not if they have lost one.

Users have to accept the terms and conditions of services and have to give permission to the apps on their mobile devices so they may use its camera, storage or microphone. Studies confirm that people tend to accept the terms of service without actually reading them (Obar & Oeldorf-Hirsch, 2018). The results of this study suggest that there may be a divergence between in-depth knowledge and an ambiguous sciolism of what actually is happening with the user's data.

Then again, there is the nothing-to-hide argument. Why bother if one has nothing to hide? One could ask these people if they have curtains in their homes. If they do, one could ask them why, since they have nothing to hide.

The problem with the nothing-to-hide argument is the underlying assumption that privacy is about hiding bad things. This biased use of the term "privacy" which is so often used interchangeably with the term "secrecy" may be a cause for the misconception that having nothing to hide is not the same as not having anything one feels they need to show someone else, either.

Significantly, there is a desire to remain anonymous on the internet and as one study (Rainie, Kiesler, Kang & Madden, 2013) suggests: 33% of adult internet users say they have used the internet in way to avoid being observed by hackers or criminals, followed by 28% who were trying to avoid advertisers, while only 5% were trying to avoid the government. Another study with the programmatic title *Why do people seek anonymity on the internet?* (Kang, Brown & Kiesler, 2013) finds that the third biggest group of interviewees seeks anonymity in order to share art or work, while the second smallest group is engaged in discussing, or is involved in politics.

With this in mind, one could theorise that people who try to share art anonymously or discuss certain topics are not looking for the "dopamine high", which social media triggers when people get likes for sharing content. As studies suggest that reward differs with respect to social networks, a study entitled *Social network modulation of reward-related signals* suggests that reward valuation in social contexts is sensitive to the distinctions of social networks, such that sharing positive experiences with in-network others may carry higher value (Fareri, Niznikiewicz, Lee & Delgado, 2012).

FREEDOM OF SPEECH ON THE INTERNET

Freedom of speech on the internet may be a benefit for citizens living in oppressive states. Moreover, during the Middle East uprisings in 2011 that would later be called the "Arab Spring", media outlets around the globe became captivated with the personal blog postings of Amina Abdallah Arraf. The freedom of writing one's opinion on the internet not only can be a benefit in favour of free press (free as in *libre*), but also bears the danger of getting away with anonymously posted denigrative statements thrown at some person, or even the manufacturing of public opinion on a large scale known as "astroturfing". This is achieved through anonymous internet comments, stories or websites that promote misinformation in an attempt to sway consumer opinion or behaviour. There are many points in support of illustrating this phenomenon. Firstly, this could be an author who writes online critiques of their own books. Secondly, it could be a restaurant-owner who writes positive reviews of their own restaurant, probably knowing that a one percent increase in the reputation score can bring about a half percent increase in occupancy and about a one and a half percent increase in revenue (Anderson, 2012). Thirdly, it could be the news which, in theory, can be manipulated and with governments seeming to have realised that forming public opinion may be one of the most powerful information weapons of the 21st century. However, let us take a step back – perhaps this does not concern freedom of speech but freedom of thought.

Bypassing the question of who should be in control, or whether there should be a controlling instance at all, one should notice the fact that before we engage with specific arguments for limiting free speech, we are in fact free to speak as we like. As a consequence, freedom of speech is different from some other types of free action.

If someone, such as the government, wants to prevent citizens engaging in certain actions – riding bicycles, for instance – it can do so by a multitude of restrictions. It can make sure that bicycles are no longer available, all existing bicycles could be burned and a ban could be placed on future imports. Freedom of speech is somehow a different case. Although one could limit the access to forms of free expression by banning books, plays and films, it is beyond one's area of authority, as well as even the possibility to make it impossible to say certain things. The only thing a government could do in such case would be to punish people **after** they have spoken.

In this line of argumentation we are, in fact, free to say anything we like. We do not necessarily have to publish it (write it on the internet), as some institution can make that freedom more or less costly to exercise. Following this line of reasoning, one may conclude that in order to **prevent** someone who has no fear of punishment from making use of their freedom of speech, one would have to remove their vocal chords. Hence, to prevent someone from exercising their freedom of thought, one would have to remove their brain. It appears that forming, influencing and directing public opinion, which in a way amounts to the same thing as to not let people think freely in the first place, seems the least drastic option while probably also being more cost effective than the former two options.

To give an illustration of what I mean, let us take a look at an episode of the British science fiction anthology series *Black Mirror*, entitled *Hated in the Nation*. In the near future, extinct bees have been replaced by robotic equivalents to maintain the balance of the ecosystem. Equipped with sensors and a script (a sequence of instructions) that is executed by a processor inside the bees, they autonomously fulfil their task nature has given them *a priori*. The government has planted a back door in the code (just in case) and the whole system is managed from one centralised headquarters. A social media movement arises where people use the hashtag "#DeathTo" adding the name and a picture of a someone slated for death, thereby giving vent to their hate of that particular person, who usually is some public figure that has become unpopular by not following the public code of behaviour. After 5 p.m., when the "polls" close, the person hated the most, namely he or she possessing the most-frequently mentioned name and that particular hashtag, gets attacked by a bee in an invasive manner and which makes its way into the brain of the victim, causing such agony that eventually leads to suicide. In the next step, the algorithm, after taking control of law enforcement, goes into a second phase, that is to say punishes all the people that had ever taken part in this social media activity (meaning they have posted #DeathTo, a name and a picture) by turning the bees against them, resulting in a multitude of deaths, thereby adding a moral value to the whole narrative.

Coupled with ingenious bits of multilayered social commentary, as well as the theoretical possibility of such a scenario occurring by considering the status of current information technology and medical research, this episode constitutes a good example in order to elaborate on the dangers

emerging from "Bridging the Bio-Electronic Divide" (see also Bridging the Bio-Electronic Divide, 2016). At this point a brief excursus is required.

"BRIDGING THE BIO-ELECTRONIC DIVIDE"

Modern efforts at "military human enhancement" draw on the fields of neuroscience, biology, genetics, pharmacology, nanotechnology and robotics. The Pentagon's high-tech Defence Advanced Research Projects Agency (DARPA) is well on the way to developing a number of prosthetic projects aimed at producing super soldiers. According to Lin, Mehlman & Abney (2013) one may divide the research on enhancement into physical capabilities, cognitive capabilities, senses, metabolism and a miscellany of dual-use research applications. Neurowarfare may be defined as warfare using "neuroweapons" that are designed to specifically target the brain or the central nervous system in order to affect the targeted person's mental state, mental capacity and, ultimately, the person's behaviour in a specific and predictable way. Psychiatry is *inter alia* based on the assumption that mental states and behaviour can be regulated or controlled with pharmaceuticals. The US military, for instance, had already become interested in "psycho-chemical warfare" back in the late 1940s. Nowadays, neuroscientific enhancement stands at the forefront of DARPA's research, including non-invasive and invasive brain stimulation, such as: brain-computer interfaces, brainwave entrainment, transcranial magnetic stimulation, intracortical microstimulation, transcranial direct current stimulation, and deep brain stimulation. Thus, by "Bridging the Bio-Electronic Divide" and with every intervention and every observation concerning every human brain, we confront a multitude of ethical issues. The moral questions related to "Bridging the Bio-Electronic Divide" concern its use as a method for modern warfare. The moral dimension has at least two different angles: (1) where does the human end and the technological begin, or what is exterior to the body of the soldier and what is interior; and (2) in which ways may the cross-linking between biological and electromagnetic enhancement potentiate the already existing "psychological" methods, such as political warfare, "psywar", institutional conflict and psychosocial combat using the great potentiality of television and the internet, all of whose primary purpose is to disorient and disarm the opposition and bear the potential to blow a state up from within. In the future, the battlefield should

be expected to shift progressively into the intellectual realm, impacting on the consciousness and feelings of many millions of people. New conflicts may no longer be wars only among people but wars of artificial intelligence and the equipment and virtual reality created by this kind of intelligence. There is a good case to believe that neurowarfare is likely to extend over many decades with the distinction between peace and war becoming not just blurred, but meaningless. The effects of combining "Bridging the Bio-Electronic Divide" with information weapons (e.g. mass media and cyber weapons) may derive – if circumstances so require – new research in neurosecurity as neuroethics. Although such weapon systems may be considered as dangerous as nuclear weapons, they will probably be more acceptable in terms of political and military ideology.

CONCLUSION

The trouble with all these developments is that one cannot go back. We are engaged in a grand social experiment, the outcome of which we can only guess at. Above all, we should keep in mind that the "smarter" our technology gets, the bigger the attack surface grows, considering all the multiple emerging side branches which every technological evolutionary step contains.

Human organisms are susceptible to infections and so are software-controlled machines, which can be infected by a virus, for instance. The underlying mechanism is the same, meaning a virus needs a host to replicate itself.

Although it seems natural to suggest that all technology should be used in moderation and in a reasonable way, there is one essential "interference factor", namely emotions. According to Phelps, Lempert & Sokol-Hessner (2014), the prevalent view of emotion and decision-making is derived from the notion that there are dual systems of emotion and reason. Making a decision often occurs in the face of uncertainty about whether one's choices will lead to benefit or harm. By contrast, the somatic marker hypothesis is a neurobiological theory of how decisions are made in the face of uncertain outcomes. This theory holds that such decisions are aided by emotions, in the form of bodily states, that are elicited during the deliberation of future consequences and that mark different options for behaviour as being advantageous or disadvantageous. This process involves an

interplay between neural systems that elicit emotional/bodily states and neural systems that map these emotional/bodily states.

DISCUSSION

We have seen that the internet was not designed to become the World Wide Web as we know it. Furthermore, we have mentioned the Big-Data-Trade-Off-Dilemma (the user trades his personal data for services or what is more, "becomes" the product eventually) and looked for possible explanations for the mindless spreading of personal data on the internet. However, there are tendencies where users seek privacy. Having said that, we have tried to deconstruct the nothing-to-hide argument fallacy. Yet the marketing divisions of Big Data corporations are doing a good job in appealing for the emotions of the users. The continuous development of something that cannot be turned off for maintenance (the internet) can be compared with replacing the engines of an airplane while flying. This continuous development makes it difficult to draw definite conclusions. With this in mind, we are constantly facing a multitude of new challenges in the field of ethics, privacy, law and security.

We have been discussing the differences between freedom of speech in contrast to the freedom of other actions (riding a bicycle in this case) and possible sanctions. In view of the lack of possibilities to control freedom of speech, which is preceded by freedom of thought, we have demonstrated possibilities of influencing public opinion. Importantly, since "Bridging the Bio-Electronic Divide" is no dystopian science fiction scenario but a potential development of the near future, further research in robot ethics and safeguarding of the emerging "smart" devices is needed. We have tried to link the feasible dangers emerging from the ingenious but malicious misuse of social media in connection with a hijacked centralised system by using the example of a contemporary and popular science fiction series.

In conclusion, it may be beneficial to educate the public as to what data is actually processed while using allegedly free (as in beer) services, since human beings may be susceptible to Alzheimer's disease, but the internet is not. Furthermore, the evident misconception of the discussion around the term "privacy" should be enlightened, since it should be treated in a neutral way, provided that studies suggest that the care for privacy is negatively connoted. The whole conception of privacy gains momentum

if we consider the possible ways of manipulating public opinion (e.g. astroturfing or military psychological warfare).

All things considered, privacy is not something one should not care about because one has nothing to hide but "privacy is the right to a free mind" (Snowden, Chomsky & Greenwald, 2016).

BIBLIOGRAPHY

Anderson, C. (2012). The impact of social media on lodging performance. *Cornell Hospitality Report, 12*(15), 6-11.

Bridging the Bio-Electronic Divide. (2016). Retrieved February 13, 2018, from https://www.darpa.mil/news-events/2015-01-19

DeNardis, L. (2014). *The Global War for Internet Governance*. New Haven and London: Yale University Press.

Fareri, D. S., Niznikiewicz, M. A., Lee, V. K., & Delgado M. R. (2012). Social network modulation of reward-related signals. *The Journal of Neuroscience: the Official Journal of the Society for Neuroscience, 32*(26), 9045-9052.

Gallagher, K. (2014). *Astroturfing: 21st Century False Advertising*. Retrieved October 14, 2018, from http://www.anniesearle.com/web-services/Documents/ResearchNotes/ASAResearchNote_2014-12_Gallagher_Astroturfing.pdf

Kang, R., Brown, S., & Kiesler, S. (2013). Why do people seek anonymity on the internet?: informing policy and design. In W. Mackay, S. Brewster, & S. Bødker (Eds.), *CHI '13 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2657-2666). New York: ACM.

Krishnamurthy, B., & Wills C. E. (2009). On the leakage of personally identifiable information via online social networks. In A. Sala, A. Goel, & K. Gummadi (Eds.), *Proceedings of the 2nd ACM workshop on online social networks* (pp. 7-12). New York: ACM.

Lin, P., Mehlman, M., & Abney, K. (2013, January). *Enhanced Warfighters: Risks, Ethics, and Policy*. Retrieved October 14, 2018, from http://ethics.calpoly.edu/greenwall_report.pdf

Michener, J. (1999). System insecurity in the Internet age. *IEEE Software, 16*(4), 62-69.

Obar, J. A., & Oeldorf-Hirsch, A. (2018, June). *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*. Retrieved October 14, 2018, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465

Ong, E. Y. L., Ang, R. P., Ho, J. C. M., Lim, J. C. Y., Goh, D. H., & Lee, C. S. (2011). Narcissism, extraversion and adolescents' self-presentation on Facebook. *Personality and Individual Differences, 50*(2), 180-185.

Palmer, D. E. (2005). Pop-ups, Cookies, and Spam: Toward a Deeper Analysis of the Ethical Significance of Internet Marketing Practices. *Journal of Business Ethics, 58*(1-3), 271-280.

Phelps, E., Lempert, K. M., & Sokol-Hessner, P. (2014). Emotion and Decision Making: Multiple Modulatory Neural Circuits. *Annual Review of Neuroscience. 37*, 264-287.

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, Privacy, and Security Online*. Retrieved October 14, 2018, from http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/

Regulating the internet giants: The world's most valuable resource is no longer oil, but data. (2017, May 6). *The Economist*. Retrieved from https://www.economist.com/news/

leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource?fsrc=scn/tw/te/rfd/pe

Ruiter, J., & Warnier, M. (2011). Privacy Regulations for Cloud Computing: Compliance and Implementation in Theory and Practice. In S. Gutwirth, Y. Poullet, P. de Hert, & R. Leenes (Eds.), *Computers, Privacy and Data Protection: an Element of Choice* (pp. 361-376). Dordrecht: Springer Netherlands.

Snowden, E., Chomsky, N., & Greenwald, G. (2016, March 25). *Snowden, Chomsky, and Greenwald discuss privacy, at 35:21* [Recorded panel discussion]. Tucson: University of Arizona College of Behavioral Sciences. Retrieved February 13, 2018, from https://vimeo.com/160952562

Wadhwa, V. (2014, April 15). Laws and Ethics Can't Keep Pace with Technology. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/