Surveillance and Censorship: Annotated Bibliography

Problem Statement:-

“The law only has sledgehammers, when what we need are parking tickets and spending tickets.”- Mitch Kapor, the cyberpunk

Nowadays, the internet has been gaining its popularity at an amazing rate. The internet has become an important communicative tool, which brings significant convenience and efficiency for people. However, the internet also has severe weakness. The internet censorship can be a protection measure. As the internet is open and comprehensive, the quality and authenticity of internet information is questionable. There are a lot of undue materials online, such as pornography and violence, which undoubtedly exerts a negative influence on people especially children physically and psychologically. Although there are several laws which regulate the illegal information and illegal activities, the laws are not complete enough to regulate all the illegal or immoral activities. It is very hard to charge a person for internet crimes, especially if the person is from a foreign website. Thus, the illegal activities and undue information are still rampant on the internet. Thus, internet censorship is needed for internet regulation. Surveillance allows governments and other agencies to maintain social control, recognize and monitor threats, and prevent and investigate criminal activity. Censorship and surveillance are intertwined on the internet, monitoring of users and communication aims at revealing the defined targets and criminalized contents and other tools and methods of censorship can be further utilized to take into action. Advanced surveillance technologies may also function as multipurpose tools. Tools of censorship and surveillance became this way bound together with the other utilities for network management.

1. Surveillance and Censorship: The Impact of Technologies on human rights Available at:- https://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf

As human lives transition online, so do human rights. The main challenge for the European Union and other actors is to transition all human rights to the digital sphere. This article argues that the human rights-based approach can be helpful in focusing discussions about security on individuals rather than states. It provides an overview of countries and companies that pose risks to human rights in the digital sphere. It lists the most relevant international laws and standards, technical standards, business guidelines, Internet principles and policy initiatives that have been crucial in transitioning the human rights regime to the digital sphere. It also analyses the impact of recent EU actions related to Internet and human rights issues. It concludes that different elements of EU strategic policy on human rights and digital policy need be better integrated and coordinated to ensure that technologies have a positive impact on human rights. The article concludes that EU should promote digital rights in national legislation of the third countries, but also in its own digital strategies.

2. Internet censorship takes new forms Available at:- file:///C:/Users/nEW%20u/Downloads/6728-Artikkelin%20teksti-15576-1-10-20120801.pdf

Censorship on the internet age has extended and become more complex. Technologies may involve contents on different levels: on web-sites, specific web-pages or even on specific words. The desired contents may be filtered out of search results or access on web pages or services may be denied. Stronger punishments include taking down the content on a given site or sanctioning the producers of the contents. Censorship and surveillance have become intertwined on the internet. Monitoring of users and communication aims at revealing the defined targets and criminalized contents - and other tools and methods of censorship can be further utilized to take into action. Advanced surveillance technologies may also function as multipurpose tools. Deep packet inspection can e.g. intercept and log Internet traffic, it may be used for enforcement of copyright, to prioritize limited bandwidth and to track users' behavior – and these tools can serve different parties and interests.

3. Geographies of Global Internet Censorship Available at:- https://www.researchgate.net/publication/227200039_Geographies_of_Global_Internet Censorship

More than one-quarter of the planet's population uses the Internet today, although access to it is highly uneven throughout the world. While it is widely celebrated for its emancipatory potential, many governments view the Internet with alarm and have attempted to limit access or to control its contents. This article seeks to provide a comprehensive, theoretically informed analysis of the geographies of Internet censorship. It begins by clarifying the reasons, types, extent of, and opposition to, government limitations of Internet access and contents. Invoking an index of censorship by Reporters Without Borders, it maps the severity of censorship worldwide and assesses the numbers of people affected, and using the Freedom House index, it correlates political liberty with penetration rates. Second, it explores Internet censorship at several levels of severity to explicate the multiple means through which censorship is implemented and resisted. The third part offers a moral critique of Internet censorship via a Habermasian interpretation of cyberspace as the closest real-world approximation of an ideal speech situation. The summary notes the paradox of growing e-government and continued fears of an expanded domain of public discourse.

4. Politics of Digital Surveillance, National Security and Privacy Available at:- https://edam.org.tr/en/politics-of-digital-surveillance-national-security-and-privacy/

Digital surveillance is a growing global concern, following the Snowden revelations, subsequent national security leaks and the most recent controversy regarding Cambridge Analytica and the Trump campaign. This article explores some of the dilemmas and deadlocks regarding digital surveillance, its extent in democracies and autocracies and how it interacts with the 'surveillance-industrial complex', SIC. SIC is an often-overlooked aspect in the surveillance-privacy debate as it is not necessarily intentions that render surveillance problematic, but its business model. In all political systems there is a secrecy, transparency and surveillance cost which drives a country's willingness to hoard secrets (citizen data, international data transfers) or to disclose some key political information to the public for the sake of legitimacy. A key component of the surveillance-privacy debate in digital space is the technology race, which drives states' unwillingness to disclose policy information due to the increasing costs of acquiring key intelligence in a networked society. Ever-increasing methods and technologies of

surveillance and circumvention alike is one of the central reasons on why efforts to regulate and safeguards surveillance mechanisms fail: they simply cannot keep up with the technologically proficient intelligence agencies, nor the ever-resourceful citizen-driven circumvention tools. The failure of surveillance transparency moves largely stem from this technological backwardness of safeguard and oversight mechanisms, as a result of which the public devises its own mechanisms to circumvent, mask or monitor how states manage and process digital intelligence and citizen data. However, especially with the growing threat of terrorism, far-right radicalization and extremist groups emerging in western societies, surveillance is viewed not only politically necessary, but also electorally popular.

5. Censorship and Secrecy, Social and Legal Perspectives Available at:- https://web.mit.edu/gtmarx/www/cenandsec.html

Secrecy and censorship involve norms about the control of information. Censorship of communication in the modern sense is associated with large, complex urban societies with a degree of centralized control and technical means of effectively reaching a mass audience. It involves a determination of what can, and can not, (or in the case of non-governmental efforts should and should not) be expressed in light of given political, religious, cultural, and artistic standards. The appearance of new communications (e.g., the printing press or the Internet) technologies invariably create demands from conflicting groups for greater openness and freedom of communication and demands for greater control. Authorities try (often in vain) to control new techniques of mass communication. Three major means of direct censorship (pre-publication review, licensing and registration, and government monopolization) are preventive in nature. Among democracies there is considerable variation in censorship by content, media of communication, place, time period and across societies. There are degrees of censorship and individual interests are balanced against those of the community, however hard the latter is to define. More common than outright prohibition, is the segmentation of material involving time, place and person restrictions. Direct government means of censorship must be considered separately from the availability of resources to create and distribute information, the activities of private groups and from informal censorship, including exclusion from sources of information and self-censorship. In a democratic society secrecy and openness exist in a continual dynamic tension.

6. Trends in transition from classical censorship to Internet censorship Available at: https://www.ifla.org/files/assets/faife/publications/spotlights/1%20Bitso_Fourie_Bothm aTrendsInTransiton.pdf

Censorship is no longer limited to printed media and videos. Its impact is felt much more strongly with regard to Internet related resources of information and communication such as access to websites, email and social networking tools which is further enhanced by ubiquitous access through mobile phones and tablets. Some countries are marked by severe restrictions and enforcement, a variety of initiatives in enforcing censorship (pervasive as well as implied), as well as initiatives to counter censorship. These trends are discussed under two broad categories of negative and positive trends. Negative trends includes: trends in issues of Internet related privacy; ubiquitous society and control; trends in Internet related media being censored; trends in filtering and blocking Internet content and blocking software; trends in technologies to monitor and identify citizens using the Internet to express their opinion and applying “freedom of speech”; criminalization of legitimate expression on the Internet; trends in acts, regulations and

legislation regarding the use of the Internet and trends in government models regarding Internet censorship; trends in new forms of Internet censorship; trends in support of Internet censorship; trends in enforcing regulations and Internet censorship; trends in Internet related communication surveillance. Positive trends include: trends in reactions to Internet censorship; attempts and means to side-step Internet censorship; trends in cyber actions against Internet censorship; trends in innovative ways of showing opposition to Internet censorship. A summary of how the trends manifest in the countries in which data were mined, as well as the trends per se is included in the article.

7. The Right to Privacy in the Digital Age Available at:- http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

In 2014 report on the right to privacy in the digital age, the former UN High Commissioner for Human Rights, Navi Pillay, contributed significantly by stating that while intrusive surveillance might be allowed, it is the responsibility of governments to demonstrate that “interference is both necessary and proportionate to the specific risk being addressed.” As meeting this condition is impossible in the case of mass or “bulk” surveillance programmes, they “may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime,” Pillay concludes. The report contributed to the revision of the Resolution on the right to privacy in the digital age by the third committee of the UN General Assembly in November of 2014, which was extended to include a call for all States to “establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data”, as well as “to provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations”.

8. Digital Activism, Internet Control, Transparency, Censorship, Surveillance and Human rights: An international perspective Available at:- https://link.springer.com/chapter/10.1007/978-94-007-5276-4_6

This Article describes, from an International point of view, the situation in different countries around the world, with particular attention to the regulation of the network on the territory, the techniques used by dissidents in loco to circumvent filters and several actions brought at state level to repress protest activities on the network. The first part of the Chapter analyzes Internet legal (and censorship) issues in the main regions of the world; the second part, with a greater level of detail, analyzes some critical situations, such as those in Cuba, Burma, Saudi Arabia, India, Syria, Iran, China, Australia, in several countries of the former Soviet Union, in the Koreas and in Vietnam, or some examples of a “freedom of information” approach, like the one that happened in Iceland.

9. Planet Blue Coat: Mapping Global Censorship and Surveillance Tools Available at:- https://citizenlab.ca/wp-content/uploads/2015/03/Planet-Blue-Coat-Mapping-Global-Censor ship-and-Surveillance-ToolsPlanet-Blue-Coat-Mapping-Global-Censorship-and-Surveillanc e-Tools.pdf

Blue Coat Devices capable of filtering, censorship, and surveillance are being used around the world. During several weeks of scanning and validation that ended in January 2013, we uncovered 61 Blue Coat ProxySG devices and 316 Blue Coat Packet Shaper appliances, devices with specific functionality permitting filtering, censorship, and surveillance. 61 of these Blue Coat appliances are on public or government networks in countries with a history of concerns over human rights, surveillance, and censorship (11 ProxySG and 50 Packet Shaper appliances). These appliances in the following locations:

Blue Coat ProxySG: Egypt, Kuwait, Qatar, Saudi Arabia, the UAE.

PacketShaper: Afghanistan, Bahrain, China, India, Indonesia, Iraq, Kenya, Kuwait, Lebanon, Malaysia, Nigeria, Qatar, Russia, Saudi Arabia, South Korea, Singapore, Thailand, Turkey, and Venezuela.

This paper supports the need for national and international scrutiny of Blue Coat implementations in the countries we have identified, and a closer look at the global proliferation of “dual-use” information and communication technologies. Internet service providers responsible for these deployments should consider publicly clarifying their function, and we hope Blue Coat will take this report as an opportunity to explain their due diligence process to ensure that their devices are not used in ways that violate human rights

10. Socio-political perspectives on surveillance and censorship: Implications for online privacy in the age of cloud computing. Available at:- https://ieeexplore.ieee.org/document/8252105

Governments interventions on the Internet have grown into importance after Edward Snowden's revelations about secret state mass surveillance programmes, along with content censorship and the partial or the complete shutdown of the Internet in times of turmoil. This paper sketches the sociopolitical perspective on State Surveillance, Censorship and Internet Intermediaries practices by evaluating the different points of view of several computer scientists, law and journalism specialists in regards to social and political implications of these interventions on individuals privacy, freedom of expression and freedom of opinion in social media and cloud computing platforms. It concludes that serious abuses of the jurisdictional power and attacks on several human rights especially freedom of expression and freedom of opinion buried using claims of threats to public order, national security, or speech defamation.