Page 228 - 239 **DOI:** *https://doij.org/10.10000/IJLSI.111271*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 4 | Issue 1

2021

Mass Surveillance: Witchcraft, Human Commodification & The Democratic State

CHHAVI PATHAK[1]

ABSTRACT

People have often discussed what a surveillance state would imply. However, with Facebook/Meta revealing its plans of creating a metaverse, a new discussion needs to be had about not just a surveillance state but also surveillance capitalism and mass surveillance. It begins with a brief analysis of witch trials as a product of pre-digital era surveillance. This paper outlines the role of surveillance in today's society and delves into its impact on human rights and democracy; while exploring the legal and social paradigms of living under surveillance capitalism. It further elaborates upon how mass surveillance is detrimental to the democratic process.

This paper firmly ascertains that Mass surveillance has led to the commodification of humans owing to an apparent lack of informed consent and massive information asymmetry. Further, Mass surveillance has led to a significant destabilization of the democratic process with attacks on whistleblowers, journalists, and opposition leaders. The quality of democracies has further deteriorated owing to the workings of companies like Cambridge Analytica and software like the spear-phishing software- Pegasus.

Keywords: *Mass Surveillance, Democracy, Informed Consent, Right to Privacy*

I. INTRODUCTION

People have often discussed what a surveillance state would look like. But now, with Facebook/meta revealing its plans of creating a metaverse, a new discussion needs to be had about not just surveillance state but also surveillance capitalism and mass surveillance.

The state manually surveilled the women, gender non-conforming people, and queer men during the witch trials and burned them alive if they behaved in a "suspicious" manner.[2] How does the new interplay between state surveillance and surveillance capitalism impact the social minorities of today?

The popular public opinion undermines the perturbing relevance of the witch hunts today and the fascinating and multifaceted history surrounding them. For a period of approximately 300 years, from the 15th century to the 17th century, an unknown number of women were

[1] Author is a Student at CHRIST (Deemed to be University) Pune, Lavasa Campus, India.

[2] Federici, Silvia. Caliban and the Witch: Women, the Body and Primitive Accumulation. New York : London: Autonomedia ; Pluto, 2003

 [ISSN 2581-9453]

executed for witchcraft. The witch hunts played a huge role in shaping the world as it exists today, which has been continuously ignored and overlooked.[3] They aided the transition from feudalism to capitalism which is often glorified and assumed to be pretty smooth. However, this could not be further from the truth. The transition was brutal; there was a significant amount of anti-capitalist resistance, women-led a significant portion of these movements.

Meanwhile, in colonies, indigenous resistance to European invaders, like the Taki Onqoy movement in Peru,[4] offered significant roles to rebellious women. These movements were deep-rooted and extremely sophisticated, and they were pretty close to achieving their goals until they were brutally suppressed. Women in medieval Europe already held a significant amount of power. They practiced pre-scientific medicine, midwifery, and other essential services using magical thinking as a self-driven technology.[5] None of the aforementioned facts aid in constructing a new economic order where everyone has to work for another.

So, to expand colonies and create a capitalist order, it was quintessential to break the power of women. For, what is the role of cisgender women under capitalism? The politically correct answer to this question would, of course, be that it is the same as men, but as history exhibits and numerous news stories till date illustrates for most of capitalist history, the role of women was to merely produce the next generation of the labor force and these witch hunts were essential to cement this role which significantly curtailed rights of women. Thus, it is evident that minorities who dare voice their opinions against authoritarian regimes are surveilled, threatened, and murdered at the hand of a state which claims to assume a paternalistic role.

A stark parallel worth examining to the witchhunts is the lynching of the Black population of the United States of America[6] or the current plight of Muslims in the Republic of India[7]. History is a testament that whenever the oppressed have resisted, the authoritative overlords have infringed upon their human rights to suppress their voices and control their actions.

What makes matters significantly more concerning is that while the witch hunts and other such events required manual surveillance to enable such atrocities, today, as mass surveillance becomes a reality, this is no longer an onerous manual task. Now, there are networks of CCTV cameras paired with facial recognition technologies, sometimes capable of detecting people's sexual orientation[8] and always able to

[3] Federici, Silvia. Caliban and the Witch: Women, the Body and Primitive Accumulation. New York : London: Autonomedia ; Pluto, 2003

[4] *Ibid*

[5] Foucault, Michel. Madness and Civilization: A History of Insanity in the Age of Reason. , 1988. Print.

[6] Beck, E. M.; Tolnay, Stewart E. (August 1990). "The Killing Fields of the Deep South: The Market for Cotton and the Lynching of Blacks, 1882–1930". *American Sociological Review*. **55** (4): 526–539. doi:10.2307/2095805. JSTOR 2095805.

[7] Abd Allāh Aḥmad Naʿīm (2008). Islam and the Secular State: Negotiating the Future of Shari'a. Harvard University Press. p. 161.

[8] Wang, Y., & Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of Personality and Social Psychology, 114(2), 246–257. https://doi.org/10.1037/pspa0000098

identify and track the citizens[9]. Furthermore, numerous states across the globe have developed *Lethal Autonomous Weapon Systems* made possible by Artificial Intelligence enabled through machine learning.[10] These technologies make non-compliant citizens not only easy to recognize but also easy to locate and anonymously target.

Thus, this paper explores how mass surveillance has led to the commodification of humans owing to an apparent lack of informed consent and massive information asymmetry infringing upon their human rights—further delving into how mass surveillance leads to destabilization of the democratic process with attacks on whistleblowers, journalists, and opposition leaders. The deterioration of the state of democracies is owing to the companies like Cambridge Analytica and software like the spear-phishing software- Pegasus.

a) Literature Review

In recent years, there has been increasing debate about mass surveillance, facial recognition technologies, artificial intelligence, and machine learning. Many have deliberated upon what it means for the marginalized and often ostracized minorities. However, with Facebook/Meta revealing its plans to create a metaverse, a new discussion needs to be had about a surveillance state and surveillance capitalism and mass surveillance. It begins with a brief analysis of witch trials as a product of pre-digital era surveillance. This paper outlines the role of surveillance in today's society and delves into its impact on human rights and democracy; while exploring the legal and social paradigms of living under surveillance capitalism. It further elaborates upon how mass surveillance is detrimental to the democratic process.

It examined findings from literary works like '***The Caliban and the Witch***' [11] , which provide a backdrop to this research, highlighting the role played by rebellious women in colonial resistance and the wide reaching consequences of the witch hunts which are often not examined when analysing these trials. Insight into the witch trials has been sought from the study conducted by ***Stuart Clark***[12] who discusses witchcraft in modern Europe in vivid detail. While, the paper by ***Walter D. Mignolo***[13] is analysed to draw upon the transition from a feudalist state to a capitalist one through movements like the Taki Onqoy movement in Peru which offered significant roles to these women. Furthermore, research by ***Beck, E. M.; Tolnay, Stewart E***[14] and ***Abd Allāh***

[9] J. Celine and S. A. A, "Face Recognition in CCTV Systems," 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT), 2019, pp. 111-116, DOI: 10.1109/ICSSIT46314.2019.8987961.

[10] Amoroso, D., Tamburrini, G. Autonomous Weapons Systems and Meaningful Human Control: Ethical and Legal Issues. Curr Robot Rep 1, 187–194 (2020). https://doi.org/10.1007/s43154-020-00024-3

[11] Federici, Silvia. Caliban and the Witch: Women, the Body and Primitive Accumulation. New York : London: Autonomedia ; Pluto, 2003

[12] Stuart Clark, Thinking with demons: the idea of witchcraft in early modern Europe. (Oxford: Clarendon Press, 1997.) Pages xviii+827. £75.00

[13] The darker side of the Renaissance : literacy, territoriality, and colonization. By Walter D. Mignolo. Ann Arbor : University of Michigan Press, 1995 . Pp. xxii+426 ISBN —0-472-10327

[14] Beck, E. M.; Tolnay, Stewart E. (August 1990). "The Killing Fields of the Deep South: The Market for Cotton and the Lynching of Blacks, 1882–1930". *American Sociological Review*. **55** (4): 526–539. doi:10.2307/2095805. JSTOR 2095805.

Aḥmad Na'īm[15] have been referred to in order to understand the experiences of minorities in the recent past.

On the flip side of the analysis is the impact of the evolution of technologies on the experiences of these minorities. Orwellian dystopias are no longer fictional. Today, there exist facial recognition technologies, as researched upon by ***Wang, Y., & Kosinski, M*** backed by machine learning so powerful they are able to detect people's sexual orientation[16] While this research has several limitations, such as only exploring a limited plethora of sexual orientations, leaving out orientations like pansexual, asexual, omnisexual, etc. it still helps highlight the legal challenge of robust machine learning tools. This paper draws upon the ***Panopticon***[17] experiment by Foucalt and Bentham to holistically examine the impact of surveillance on the human psyche. It then delves into the ***case of cambridge analytica*** and politics in an era of mass surveillance [18][19] and ***surveillance capitalism***[2021].

Moreover, this paper examines Mass surveillance is detrimental to the citizens' right to privacy and often leads to infringement of their civil and political rights in light of the ***Watt, Eliza***[22]. Such surveillance is usually carried out by using tactics that allow the entity to gain access to bulk communications through Informant networks, CCTV Networks paired with artificial intelligence, User action logging, mass hacking through techniques like phishing, spear phishing, conducting mass interception of communications, making indiscriminate use of facial recognition technologies, Cookie pooling and making use of mobile phone trackers[23].

b) Objectives

The study was geared to achieve the following objectives:

- To outline the role of surveillance in today's society
- To analyze human rights under a surveillance society

[15] Abd Allāh Aḥmad Na'īm (2008). Islam and the Secular State: Negotiating the Future of Shari'a. Harvard University Press. p. 161.

[16] Wang, Y., & Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. Journal of Personality and Social Psychology, 114(2), 246–257. https://doi.org/10.1037/pspa0000098

[17] Michel Foucault, Discipline and Punish Jeremy Bentham, Panopticon http://www.fcsh.unl.pt/docentes/rmont... [accessed 01 November 2021]

[18] Ünver, H. Akın. Politics of Digital Surveillance, National Security and Privacy. Centre for Economics and Foreign Policy Studies, 2018, http://www.jstor.org/stable/resrep17009.

[19] Manning, Peter K. "Surveillance and Democracy." The Canadian Journal of Sociology / Cahiers Canadiens de Sociologie, vol. 36, no. 3, Canadian Journal of Sociology, 2011, pp. 241–45, http://www.jstor.org/stable/canajsocicahican.36.3.241.

[20] Shoshana Zuboff,The Age Of Surveillance Capitalism: The Fight For A Human Future At The New Frontier Of Power

[21] Fuchs, Christian. "Karl Marx in the Age of Big Data Capitalism." Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data, edited by Christian Fuchs and David Chandler, University of Westminster Press, 2019, pp. 53–72, http://www.jstor.org/stable/j.ctvckq9qb.6.

[22] Watt, Eliza (2 September 2017). "'The right to privacy and the future of mass surveillance'". The International Journal of Human Rights. 21 (7): 773–799. doi:10.1080/13642987.2017.1298091. ISSN 1364-2987. S2CID 148928418.

[23] Ben Underwood, Hossein Saiedian,SECURITY AND PRIVACY Volume 4, Issue 2 e142 Mass surveillance: A study of past practices and technologies to predict future directions Mass surveillance: A study of past practices and technologies to predict future directions

- To analyze the legal and social paradigms of being living under surveillance capitalism
- To critically examine the democratic process under mass surveillance

c) Hypothesis

The following hypotheses will be examined in this study:

- Mass surveillance is likely to lead to the commodification of humans owing to an apparent lack of informed consent
- Mass surveillance is likely to eliminate democracy in its truest form

II. THE AMBIT OF MASS SURVEILLANCE

Mass surveillance is the name given to a complex network of surveillance of a substantial population[24]. Mass surveillance may be carried out by governmental organizations, corporations on behalf of governments, or corporations on their initiative. Many authorities carrying out such mass surveillance have mentioned that it is necessary to combat terrorism, reduce crime, control social unrest, and protect the nation's national security interests[25]. Mass surveillance is distinct from targeted surveillance, and depending on each nation's legal framework dealing with it, the legality behind mass surveillance may vary.

Mass surveillance is detrimental to the citizens' right to privacy[26] and often leads to infringement of their civil and political rights[27]. Such surveillance is usually carried out by using tactics that allow the entity to gain access to bulk communications through Informant networks, CCTV Networks paired with artificial intelligence, User action logging, mass hacking through techniques like phishing, spear phishing, conducting mass interception of communications, making indiscriminate use of facial recognition technologies, Cookie pooling and making use of mobile phone trackers[28].

Global mass surveillance can be observed since the communications surveillance sharing agreement in the mid-1940s called UKUSA[29]. This agreement was initially between Britain and the United States. However, it has expanded to include Canada, Australia, and New Zealand and is often referred to as the five eyes agreement[30]. The Five Eyes countries cooperate with various third-party countries to increase the scope of surveillance[31]. The "Nine Eyes" is an extension of the agreement with third party nations consisting of the Five Eyes plus Denmark, the

[24] Ben Underwood, Hossein Saiedian,SECURITY AND PRIVACY Volume 4, Issue 2 e142 Mass surveillance: A study of past practices and technologies to predict future directions Mass surveillance: A study of past practices and technologies to predict future directions

[25] "Mass Surveillance". Privacy International; https://privacyinternational.org/learn/mass-surveillance

[26] Watt, Eliza (2 September 2017). "'The right to privacy and the future of mass surveillance'". The International Journal of Human Rights. 21 (7): 773–799. doi:10.1080/13642987.2017.1298091. ISSN 1364-2987. S2CID 148928418.

[27] *Ibid*

[28] *Supra* note 22

[29] "Declassified UKUSA Signals Intelligence Agreement Documents Available" (Press release). National Security Agency. 24 June 2010

[30] Cox, James (December 2012). "Canada and the Five Eyes Intelligence Community" (PDF). Canadian Defence and Foreign Affairs Institute.

[31] *Ibid*

Netherlands, Norway, and France[32]. The "Fourteen Eyes" or SIGINT Seniors Europe (SSEUR) consist of the "Nine Eyes" as well as Sweden, Belgium, Italy, Spain, and Germany[33].

Despite being a pioneering agreement, the UKUSA today is far from the only such agreement. In 2013, documents released by Edward Snowden revealed how the "Five Eyes are surveilling several intergovernmental organizations, diplomatic missions, and government ministries." With reference to India, the papers revealed how the Embassy of India in Washington, D.C. and the Permanent Representative of India to the United Nations had gained access to the information of Indian citizens by Copying entire hard disk drives and picking data from screenshots [34].

III. MASS SURVEILLANCE AND INFORMED CONSENT

Prior to any contract being legally enforceable, the principle of consensus ad idem must be adhered to. However, the principles of contract law in this regard appear archaic. They were not developed considering the emerging technicalities of cyberspace. The meeting of the minds as envisaged under the principle of consensus ad idem poses a complex legal challenge when dealing with standard forms of contract spread across the internet.[35]

Discussions about prevalent forms of contract on the internet or e-contracts revolve around three primary types of e-contracts. These are browsewrap contracts, shrink wrap contracts, and Clickwrap or click-through contracts.[36] Websites using a browsewrap contract maintain that continued use of the website by a user is deemed to be acceptance of its terms of use and other policies. This type of contract is usually used when the website's terms of service are updated. Shrinkwrap contracts are usually used in software licensing agreements. Here, the term 'Shrink Wrap' represents the shrink wrap plastic wrapping that coats software boxes or the terms and conditions that come with products on delivery. Clickwrap or click-through contracts mandate that the user indicates consent to the terms and conditions or terms of service by clicking the "ok" or "I agree" button on a dialogue box. Users may choose to either accept or reject the terms, but they would not buy or use the service following such rejection.

No concrete judicial precedents pertaining to the validity of these agreements can be found in India. However, the Information Technology Act, 2000[37] , and the Indian Evidence Act, 1872[38]provide some recognition and regulation

[32] Top Level Telecommunications, Five Eyes, 9-Eyes and many more Archived 18 December 2013 at the Wayback Machine

[33] Top Level Telecommunications, 14-Eyes are 3rd Party partners forming the SIGINT Seniors Europe Archived 19 January 2014 at the Wayback Machine

[34] Shobhan Saxena (25 September 2013). "NSA planted bugs at Indian missions in D.C., U.N." The Hindu. Chennai, India.

[35]Kapoor, R., 2022. Avtar Singh's Law of Contract & Specific Relief. 13th ed. EBC, pp.68-70.

[36] Hillman, R. A. (2017). CONSUMER INTERNET STANDARD FORM CONTRACTS IN INDIA: A PROPOSAL. National Law School of India Review, 29(1), 70–85. http://www.jstor.org/stable/26459201

[37] Section 10, Information Technology Act, 2000, Act 21 of 2000

[38] Section 65B,85A, 85B, 85C, 90A Indian Evidence Act 1872, Act 01 of 1872

to E-Contracts. The Information Technology Act [39]incorporates intricate conditions for attribution, acknowledgment, and dispatch of electronic records and secured electronic procedures. It also determines that communication of proposals, acceptance of proposals, revocation of proposals and acceptances, may be expressed in electronic form or by utilizing an electronic record. This would not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

There are many limitations that pertain to these contracts, like the fact that most users accepting the terms do not read the clauses thoroughly. However, the main drawback of such standard e-contracts can be prudently inferred from the judgment delivered in a case dealing with standard forms of contracts. In the present case,[40] the Apex Court maintained in relevant part that there would be no scope for the weaker party to negotiate the terms of the contract in a standard form of contract. The weaker party accepts or rejects the service or goods in such a contract. In other words, their choices are limited to either accepting unreasonable or unfair terms or refraining from using the service forever.

These aforementioned limitations of e-contracts illustrate the problem of informed consent. When the websites enforce the terms of these agreements, they can access data which had the user been made more holistically aware of the terms they would not have agreed to share. This may include location data, body sensor data, contacts, Microphone logs, Call logs, Camera logs, and the like.

These data collection initiatives have created a sort of data economy raising various issues in the legal domain as the legal framework attempting to govern this permits the creation of data logs and promotes it. This can be inferred through Rule 4(1)(a),4(1)(b),4(1)(c),4(1)(d) of the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021[41] which require the appointment of Chief Compliance Officer to ensure compliance with these rules, appointment nodal contact person for round the clock coordination with law enforcement agencies submission, the appointment of a Resident Grievance Officer, a resident of India required to fulfill the aforementioned rules and publication of monthly "compliance reports" regarding all complaints received, action taken, action taken thereon, and the number of specific communication links or parts of information that the intermediary has removed or disabled access to respectively. This apparent limitation of these policies around the data economy cis often dismissed from discussion a famous statement frequently brought up is "If you do not have anything to hide, why are you worried?"

[39]Information Technology Act, 2000, Act 21 of 2000

[40] Delhi Transport Corporation v. DTC Mazdoor Congress, 1991 Supp (1) SCC 600, ¶280 (SCI); See Eike Von Hippel, "The Control of Exemption Clauses – A Comparative Study", 16(3) International and Comparative Law Quarterly 591 (1967)

[41]Rule 4(1)(a),4(1)(b),4(1)(c),4(1)(d) Ministry Of Electronics And Information Technology Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021

However, while this statement might seem like an end-point of the conversation, it should be considered the very start of the conversation surrounding data protection. Suppose the government decides to table a bill stating that every person would be assigned another person watching over them. Most citizens, particularly the ostracised minorities, would heavily oppose this bill. It would be horrible- people would not be able to oppose the government in any manner. They would not hold meetings, protests, and civil society activity would essentially no longer exist. 24/7 surveillance mandated by these rules is no different[42]

A common argument against this presentation of facts is that government agencies do not hold the data collected by these "private actors" who merely publish it to the government for better security of citizens. However, these rules irreversibly weaken the scope of the KS Puttaswamy [43]judgment, making it impossible for intermediaries to protect user data from government actors. The rules have also essentially overturned the intermediary liability protected by the Supreme Court in Shreya Singhal vs. Union of India[44]. They damage the holding by stating that an "unlawful act" in S.79 of the Information Technology Act, 2000[45] must be limited by Art 19(2) of the Constitution[46].

Further, data collection by private entities should also be a cause of concern as, unlike government actors, private entities are not even elected representatives of the people. Mass surveillance by these entities also disrupts the Rule of Law. Suppose the Data Collected by these private players does not harm anyone. It still creates a situation of information asymmetry where one party knows everything about the other. In contrast, the other party does not even know who that party is. In a society divided by this gap in information, the rule of law, the most primary of rights in a post-modern nation, can never be realized. Without the Rule of Law, no right can exist

A significant rebuttal to this point is well; the machines collect data, not individuals. It is not the person under surveillance; it is their "Data Double." A mere culmination of your activity. However, this appears to be pure psychological bias, as a machine can gather significantly more data than any human. The "Data Double" is a mere construct. It faces no consequences of data-harvesting schemes. An individual surveilling an individual through the location history derived from the cab-for-hire application will not cause any harm to a "Data Double." Still, the actual person is likely to face the consequences.

Another aspect of this can be understood from the works of the upon the consequences of the panopticon. The panopticon was a prison system model that barred prisoners from engaging in misconduct through the mere threat of surveillance. It contained a central observation tower placed within a circular arrangement of

[42] *Ibid*
[43] Justice K.S.Puttaswamy(Retd) vs Union Of India CIVIL) NO. 494 OF 2012
[44] Shreya Singhal v. Union of India AIR 2015 SC 1523
[45] Section 79, Information Technology Act, 2000, Act 21 of 2000
[46] Article 19(2), The Constitution of India [India], 26 January 1950,

prison cells.[47] From the tower, a guard could potentially watch every cell, but the inmates could not see into the tower. Prisoners will never know whether or not they are being surveilled. This was used as a disciplinary mechanism in societies to subjugate its citizens. This caused signs of panic to grow among the prisoners, as they developed severe

While Foucault did not look at the digital structure of today, he did look at the use of power and its increasing bureaucratization in the modern world, studying torture and its consequences. Today, the panopticon can be used to examine the impact of surveillance in various settings like government administration, modern workplaces, and consumer contexts. Nevertheless, the importance of the panopticon as a metaphor for mass surveillance begins to diminish when one realises that today, mass surveillance on the internet is almost impossible to locate. It is invisible, with no visual marker like a central tower, nor supervisor staring there every time one log into a webpage. The user clicks away on the internet trackers on the internet staer unveiling and linking different domains of user history. This can be observed through companies like Wayfair calling users the moment they click on their website.[48] These companies work with a number of other third-party trackers like the retargeting company Criteo and Tealeaf, an analytics company by IBM. It also lists so-called trackers from tech giants like Google, Facebook, Snapchat, Microsoft's LinkedIn, and more.[49]

This implies that the user becomes a product, and the mega-corporations running targeted advertisements through cross-site tracking become the actual consumers. [50]A potential solution suggested to deal with corporations essentially treating users as a product under surveillance capitalism is to pay users for their data.[51] However, this implies that companies like Facebook would develop policies where the users either pay to access their sites or give them rights over their data. This would broaden the digital divide and disproportionately impact lower economic classes.

Revamping the policies surrounding the Data Economy, especially when it comes to mass surveillance, is a difficult task that requires significant human rights considerations, technical knowledge, and an in-depth analysis of the socio-political consequences of the same. Nonetheless, it is also a task that requires urgent efforts to help protect the interests of the citizens.

IV. MASS SURVEILLANCE AND DEMOCRACY

Edward Snowden's contribution in highlighting the level of surveillance in 2013 helped shed light

[47] Rosen, David, And Aaron Santesso. "The Panopticon Reviewed: Sentimentalism And Eighteenth-Century Interiority." Elh 77, No. 4 (2010): 1041–59. Http://Www.Jstor.Org/Stable/40963119.

[48] Graham, M., 2022. How brands get your phone number and call after they see you on their website. [online] CNBC. Available at: <https://www.cnbc.com/2019/11/07/how-brands-get-your-phone-number-and-call-when-they-see-you-browsing.html>

[49] *Ibid*

[50] Zuboff, S., & Schwandt, K. (2019). The age of surveillance capitalism: the fight for a human future at the new frontier of power.

[51] *Ibid*

upon what surveillance means for democracy in a nation.[52] As they are understood today, his disclosures reveal that general surveillance is incompatible with the human rights framework understood to be a quintessential component of a democracy. Mass surveillance notes down citizens' every action, often making them censor and limit themselves. This can be understood by examining the condition of dissidents, journalists, and their sources in nations using mass surveillance tactics.

Governmental transparency is quintessential for the well-being of any democratic nation-state. However, as states make laws to weaken transparency like the 2019 amendment to the RTI Act in India, this transparency is broken[53]. Thich lack of transparency amongst various organs of the government often forces people to become whistleblowers and inform the general public about the activities of the state. Take, for example, the 2019 public increments of information released by numerous whistleblowers about Trump's attempt to shake down the president of Ukraine.[54] But surveillance is capable of breaking this method of creating transparency with whistleblowers and activists being surveilled, harassed, and even murdered[55].

The impact of mass surveillance on democracy can further be analyzed through the case of Cambridge Analytica. In 2018, it was noted that Cambridge Analytica gained access to and exploited the personal data of Facebook users. [56] The company could launch massive virtual campaigns on Facebook using the acquired information. Various news outlets documented that it essentially ran all of Trump's 2016 digital campaign.[57]

In India, Cambridge Analytica has reportedly been used by the Indian National Congress to conduct an "in-depth electorate analysis" at various points of time, including the 2010 Bihar Legislative Assembly elections[58]. Moreover, it has been alleged that the company had offices located in India and that the INC party was a significant client[59] to subvert Indian voters away from the Bharatiya Janata Party as part of a neocolonial effort to undermine Indian politics[60].

More recently, a spear-phishing software by the NSO group called Pegasus made headlines for similar reasons.t infiltrates the devices using Zero Click Technology. This means that Pegasus can install malware on any device without the need to click the attachment or link.[61] It attacks the device while remaining virtually

[52]Burrough, Bryan; Ellison, Sarah; Andrews, Suzanna (April 23, 2014). "The Snowden Saga: A Shadowland of Secrets and Light". Vanity Fair.

[53] Guha, Abhijit. (2019). Article on RTI Amendment The-Statesman-29-08-2019-page-14.

[54] Mazzetti, Mark; Benner, Katie (September 30, 2019). "Trump Pressed Australian Leader to Help Barr Investigate Mueller Inquiry's Origins". The New York Times.

[55] *Supra* Note 51

[56] Doward, Jamie; Cadwalladr, Carole; Gibbs, Alice (4 March 2017). "Watchdog to launch inquiry into misuse of data in politics". The Guardian. ISSN 0261-3077.

[57] *Ibid*

[58] Punit, Itika "Cambridge Analytica's parent firm proposed a massive political machine for India's 2014 elections". Quartz. Reuters.

[59] "'Believe' Congress was a client, says Cambridge Analytica whistleblower". The Economic Times. 27 March 2018.

[60] "BBC documentary clip goes viral, shows Congress poster in office of Cambridge Analytica's ex-CEO Alexander Nix". DNA India.

[61] Boot, Max. "An Israeli tech firm is selling spy software to dictators, betraying the country's ideals". The Washington Post.

undetectable. Pegasus is particularly efficient in its capability to exploit "Zero-Day Vulnerability." [62]A Zero-Day Vulnerability is any software security flaw like a bug or defect in the Operating System that the manufacturers are yet to discover. If it has been found, it has not been patched yet. Unlike traditional spear-phishing tools, it can Jailbreak iOS devices and gain root control over android systems.[63]

It employs a sophisticated command-and-control (C&C) infrastructure to deliver exploit payloads and send commands to Pegasus (s).[64] There are four known tediums of the C&C infrastructure or the Pegasus Anonymizing Transmission Network (PATN). Each contains 500 domain names, DNS servers, and other network infrastructure. The PATN allegedly registered high port numbers for their online infrastructure to avoid conventional Internet scanning. PATN also uses up to three randomized subdomains unique per exploit attempt and randomized URL paths. It reveals information like the targeted user's location, call logs, notes, location activity, and anything else the controlling server desires. [6566]In India, it was found that the government had deployed the Pegasus Project on numerous opposition leaders, ministers, campaign advisors, activists, judges, journalists, religious leaders, Election Commissioners as well as individuals heading the Central Bureau of Investigation (CBI)[6768]Relevant agencies subsequently investigated many of the phones belonging to the revealed names, and it was confirmed that they had been targeted by the Pegasus spyware.[69]

While all these events led to massive investigations set out by various states, the center and the Apex Court in India most yielded no significant outcome in protecting the Right to Privacy of these citizens. These technologies have time and time again been used to undermine the democratic process by foreign and national agencies.[70] They create a situation of information asymmetry, undermining the principle of the rule of law and infringing upon the human rights of citizens.

V. CONCLUSION

Witch trials are an often overlooked yet immensely influential example of an overreach of power by the state made possible by mass surveillance. The state manually surveilled the women, gender non-conforming people, and queer men during the witch trials and burned them alive if they behaved in a "suspicious" manner. Thus, the conversation around a

[62] Bouquet, Jonathan. "May I have a word about… Pegasus spyware". The Guardian.
[63] John Snow (August 17, 2017). "Pegasus: The ultimate spyware for iOS and Android". Kaspersky Daily.
[64] *Ibid*
[65] *Ibid*
[66] Marczak, Bill; Scott-Railton, John . "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender". Citizen Lab.Amitai Ziv "Israeli Cyberattack Firm NSO Bought Back by Founders at $1b Company Value; Two founders are partnering with European private equity fund Novalpina to purchase the controversial firm from Francisco Partners"
[67] "Phones Of Indian Politicians, Journalists Hacked Using Pegasus: 10 Facts On Report". NDTV.
[68] "Pegasus spyware used to 'snoop' on Indian journalists, activists". The Hindu. Special Correspondent. J. ISSN 0971-751X.
[69] "Eleven phones targeted: Of woman who accused ex-CJI of harassment, kin". The Indian Express
[70] "Leaked Snoop List Suggests Surveillance May Have Played Role in Toppling of Karnataka Govt in 2019". thewire.in.

surveillance state and its limitations is in no way a new one.

Delving into the witch trials as a product of pre-digital era surveillance. This paper firmly ascertains that Mass surveillance has led to the commodification of humans owing to an apparent lack of informed consent and massive information asymmetry infringing upon the human rights of citizens. Further, Mass surveillance has led to a significant destabilization of the democratic process with attacks on whistleblowers, journalists, and opposition leaders. The quality of democracies has further deteriorated owing to the workings of companies like Cambridge Analytica and software like the spear-phishing software-Pegasus.

The government legislation, policies, and rules have failed to protect the citizens' privacy; they have aided the infringement of the Fundamental Right to Privacy. There is an apparent need for better protection of the Right to Privacy, which forms the foundation of all other rights in the digital era.

*****