Machine Learning and Artificial Intelligence: The World's Panopticon

A Research Paper Submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Prithvi Kinariwala

Spring 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

I: Introduction to Machine Learning and Artificial Intelligence in Censorship and Surveillance

For centuries, surveillance and censorship have been at the crux of national security operations. Espionage for military purposes dates back to at least the 4th century BC, where the practice was quoted in Sun Tzu's *Art of War.* As technologies evolve, so do a nation's surveillance and censorship techniques. The recent advent of machine learning (ML) and artificial intelligence (AI) have given governments significant capabilities to both spy and control their citizens.

Janiesch et. al. (2021) define ML as "the capacity of systems to learn from problem-specific training data to automate the process of analytical model building" (p. 1). While traditional algorithms take in a set of instructions and data and output a distinct result, ML applications take in data and the result and return an algorithm that becomes more accurate without being explicitly programmed to. AI is widely referred to as ML applications where machines are taught to perform with "human-like" intelligence. Image recognition is one common ML application. Images with known characteristics are used to train models to classify images with unknown objects.

Today, nations that employ ML/AI-based surveillance and censorship have significant overreach into the lives of their citizens. The academic consensus around ML/AI-based surveillance claims it's much more powerful than its non-ML/AI counterpart. Adding another level of complexity, nations that do currently use ML/AI solutions use it to varying degrees in terms of infringing on citizens' lives (Feldstein, 2019). Governments today, like those of the US and China, use such technologies indiscriminately, despite concerns on its ethicality.

Global surveillance and censorship have long been sociotechnical systems concerning people across the world. According to Gellman & Adler-Bell (2017, p. 2), the ability for nations

to see deep into the lives of its citizens as well as stop the spread of free information has often been perceived to be used "heaviest in communities already disadvantaged by their poverty, race, religion, ethnicity, and immigration status." The concrete manifestation of this targeted heavy usage is used in blunter situations involving "stop-and-frisk" and "suspicionless searches." Stoycheff et al. (2018, p. 603) compare this control to a *panopticon* or a "theoretical prison design in which inmates know they may be monitored but are unable to discern exactly when." Many claim this ability "is believed to function as the ultimate mechanism of social control" (p.603).

For that reason, there truly isn't a difference in the extent of the abuse of ML/AI for these purposes between nations like China and the US. However, it's the extent of access these nations have to the data of their people that determines how successful the countries are at using such technologies. Using sociotechnical methods to dissect the social ramifications between the two nations' use of ML/AI, this paper will use the frameworks of Actor-Network-Theory, technical-attitudes, and *engineering as experimentation* to show that the "democraticness" of a nation does not necessarily correlate with lesser surveillance and spying. Finally, this paper will address potential alternate solutions nations should employ to better protect their citizens.

II: Consequences of the Proliferation of ML/AI Surveillance and Censorship

It's well known that nation-states incorporate ML/AI surveillance into their national security policies for both domestic and foreign use. Whistleblowing incidents like Edward Snowden's NSA scandal underscore the claim that the technology's use is an infringement of personal liberties. In general, ML algorithms perform better with greater data. This pushes nations to collect more data from their citizens. Amongst citizens trying to avoid government surveillance and censorship, some have begun to use new and emergent technologies to avoid detection. One example is Tor, or The Onion Router, a network utility allowing users to use

numerous encrypted routers to obsecrate both themselves and their intended server. Named relays, these routers provide protection and anonymity for both the client and server using Tor for communications. Tor's relay workings are illustrated in Figure 1. Aminuddin et. al (2018) assert with the advent of "machine learning classification technique similar to the classification of encrypted traffic on the surface web" (p. 113), many fear that governments can employ machine learning to crackdown and prosecute users of Tor.

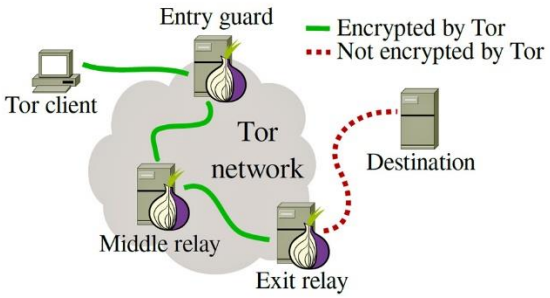

Figure 1. Overview of a Tor network with relays.
The figure shows Tor Clients using encrypted networking to maintain anonymity (Goodin, 2014, n.p.).

One of the greatest consequences of this of global ML-based surveillance proliferation is a new arms race nations across the world are embroiled in, with each vying for greater intelligence on other world powers. Petit (2019) draws upon this proliferation to show governments have begun to use "global surveillance a face and a name" of an "everywhere war" (p. 30). This everywhere war poses multiple threats for humans, namely, with the extreme over-surveillance of people. Feldstein, S. (2019, n.p.) claims that China and the United States are proliferating the world with AI-based surveillance systems. However, when power is given to Autocratic and semi-autocratic nations, they seem to "exploit AI technology for mass surveillance purposes." As mentioned in the China case study, the Xinjiang region, information is "systematically collect[ed] information on its citizens" by the Chinese Communist Party

(Leibold, 2019, p. 47). A concern raised by this case study would be what social factors specifically in China impact the ability of governments to attain and maintain such control over their subjects? This question is derived especially from Leibold, J. (2019, p. 52), where the author mentions that specific cultural differences between China and Western countries are the reason why such surveillance can never happen in more democratic countries.

On a more social scale, studies have been conducted in the realm of surveillance and the police-state. McCahill, M. (2007). Cites "disproportionate targeting and exclusion" (p. 14) due to technologies having inbuilt sensitives for marginalized people. Biases and insensitivities in algorithms are linked to a denigration of personal rights and individuality. Aside from government ML/AI usage, similar trends are apparent with the technology's use in the private sector. Across the globe, experts foresee a weakening of personal self-determinism due to the overuse of AI around normal citizens. Larrondo, M. E., & Grandi, N. M. (2021, p. 4) claim technology giants like Twitter and Facebook use this AI technology for questionable use with citizens—further pushing individuals to question the use of AI as a service to people.

To hinder this expanse of abuse, fair use agreements of ML and AI technologies have existed in the past. However, they need to be methodically checked to ensure they do not become abused past their usage. Preece et al. (2018, p. 42) describe fair use of ML and AI. The paper states organizations recently have begun to share information and technology strategies with the use of "coalition agreements" (p. 40). The newest technologies included in these agreements are ML and AI applications. However, these solutions pose their issues of both "robustness and interpretability" (p. 40). ML applications can become too robust—meaning they can become extremely powerful yet still not be completely correct. On the other hand, they can become too interpretable, or "the need for services to offer explanation facilities to engender user trust" (p.

40). Because of this inability of completely accurate, organizations are reluctant of sharing the ML/AI solutions in surveillance.

There is also a lack of clarity in the social impacts of life under ML/AI surveillance and censorship. Do other ML/AI usages in the lives of people also become over-corrective and thereby too powerful? Llansó (2020, p. 1) indicates that content filtering powered by AI often censors information that isn't meant to be censored. The author states, "Missing from [AI technology] promises, however, is an acknowledgment that proactive identification and automated removal of user-generated content raises problems beyond issues of "accuracy" and "overbreadth."

These concerns outline issues with the use of ML and AI in surveillance-based situations. Despite being potentially extremely powerful, the technology is also significantly volatile. The use of the technology by China and the US illustrates the issues of such technology in the hands of all governments: democratic or not. Instead of just looking at the use of the technologies by the two nations, there needs greater emphasis on sociotechnical implications of such use.

III: Dissecting ML/AI with Sociotechnical Methods

Sociotechnical systems are best described by addressing not just the engineers and devices in a system, but also the interactions between the actors. This relationship is commonly referred to as Actor-Network Theory (ANT). Created by Bruno Latour, Michel Callon, and John Law, ANT suggests that an actor-network contains not only people but their respective organizations and objects within the organizations, as well as their respective interactions. These networks are always subject to change and adapt to changes in the actors. ANT can be used to identify how human and non-human actors play into the world of ML and AI-based surveillance in a manner not easily seen before. Actors can be national-level organizations, like the National

Security Administration (NSA) or Russian FSB; technologies, like ML/AI and cultural practices, like submission to government surveillance measures. Bruno Latour in "Where are the missing masses?" (1992) explains "how artifacts can be deliberately designed to both replace human action and constrain and shape the actions of other humans" (p. 151). The best application to this context would be how censorship technologies are bound to modify the behavior of citizens worldwide. By any measure, the current state of surveillance and censorship is as much a geopolitical issue as it is represented by actor-network theory. China and the United States are key actors, alongside the technologies they possess and the allies they support.

Addressing another framework, Kerschner & Ehlers (2016, p. 143) suggests that there exists a broad spectrum of people's attitudes on new technologies. Researchers' "technoattidues" can be split into enthusiasm, determinism, romanticism, and spectisism. This framework works with the cultural aspect of problem mapping. Having citizens map how dangerous they find governments using ML and AI for surveillance and censorship can be utilized as means of sociotechnical introspection. Figure 2, adapted from Kerschner & Ehlers (2016), illustrates these main distinctions in attitudes as well as components of the attitudes.

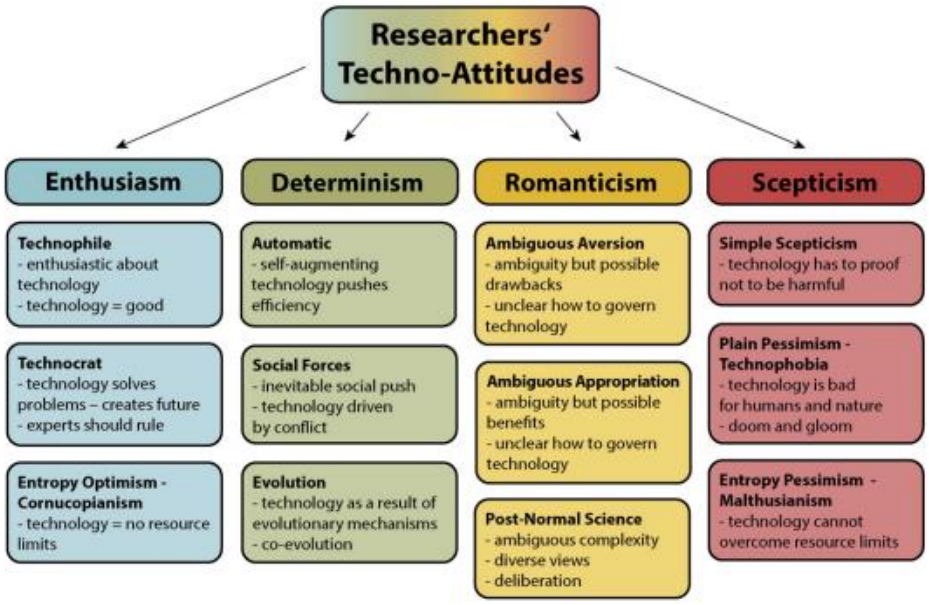

Figure 2. Breakdown of Researchers' Techno-Attitudes.
This chart shows how Enthusiasm, Determinism, Romanticism, and Skepticism are part of Techno-Attitudes.
(Kerschner & Ehlers, 2016)

The first attitude, enthusiasm, is the extent that technology is considered inherently good and its misuses accidental" (p.144) Many technophiles believe that problems "which are detrimental to human goals, can be effectively removed or overcome by technology" (p.144). The next attitude, determinism, includes the idea that technology is driven by conflict and social push. This too can be applied to global adaptions of surveillance technologies. Next, romanticism, itself split into ambiguous aversion, ambiguous appropriation, and post-normal science covers the "middle ground between technology enthusiasm and skepticism" (p.145). Finally, skeptic attitudes claim "technology can undermine social cohesion, foster individualization, and isolation" (p.147). Such concepts of thinking date back to ancient times, where technology was regarded with great suspicion as "it bore the danger of being turned away from God or the gods until it had been established that technology was innocent or necessary" (p.147). All four of these attitudes help tremendously when gauging government use of ML and

AI in surveillance and censorship as there are significant cultural differences between nations like China and the US.

One of Kerschner's primary concluding remarks was that a technologically driven society "can only engage in constructive deliberation on the use of technologies, if we know on what framings of technology the relevant research rest" (p.148). Albeit a general statement, paying attention to whether or not surveillance and censorship technologies are transparent enough is also significant to accessing the various implementations of the technologies by nations.

Both ANT and Researchers' techno-attitudes allow for the analysis of the societal dangers of overextending ML/AI technologies; specifically, by national governments. Referencing again the case studies from countries around the world, there are sets of distinct attitudes in each respective nation. Techno-attitudes builds a direct model that will be used to access national implementations of the overreach of governments utilizing machine learning and artificial intelligence in surveillance and censorship.

Martin and Schinzinger (2004) claim engineering work is often experimental with the greater populous being subjects of said experimentation. Citing the examples of the Titanic and Challenger, the authors claim engineering tests technologies upon unknowing people. Citizens now are facing censorship and surveillance to an extent never before possible only because of the capabilities afforded to them by machine learning and artificial intelligence. Although certain nations—like China in the Xinjiang region—"experiment" more with these new technologies, it's widely accepted that the new technologies offer a vision into people's lives that was not possible before.

All three frameworks: Actor-Network Theory, technical attitudes, and engineering as experimentation can be applied to each country that uses machine learning and artificial

intelligence for surveillance and censorship. Due to the sheer complexity and controversy of the technology, these three methods can give great insight into the sociotechnical inner workings of each country.

III: Social Consequences of ML/AI Censorship and Surveillance

In June 2013, the world was stunned by whistleblower Edward Snowden's leaks. Showing the world that the United States' NSA habitually performed illegal surveillance, Snowden brought scrutiny to an agency tasked with keeping America safe. One example of this surveillance was the collection and monitoring of telephone records and texts of its citizens—a gray legal area. He also revealed that the NSA tapped into the servers of tech giants like Apple, Google, and Facebook, to spy on audio and video chats, photographs, and emails. Although Snowden did not reveal the direct use of ML and AI within NSA's surveillance networks, he did stifle consensus and brought scrutiny to the surveillance practices of the US. Most importantly, Snowden's story shows that even self-proclaimed "democratic" nations are entrenched in somewhat shady surveillance and censorship behaviors (Verhelst et al, p 2976, 2020).

In the context of government-based ML/AI surveillance and censorship, "results" are defined to where each nation falls on the socio-technical frameworks outlined earlier. Each framework assesses a unique combination of assessing personal liberties, the population's attitudes, and finally, the indirect negative repercussions of government ML/AI surveillance and censorship. Due to the varying nature of how nations use such technologies, the methods outlined give a greater dissection of the causes and effects of the use of ML/AI surveillance and censorship into peoples' lives. Comparing both China, a nation known for strict national governance and lack of public liberty and the United States, a nation that claims its citizens have the most civil liberties, a common trend can be noticed.

Kerschner makes the point of Determinism as an attitude (p. 143, 2016). Determinism itself is broken into three aspects: “Automatic,” or how technology pushes efficiency; “Social Forces,” or the relationship between social pushes and technology; and “Evolution,” or how technology is a result of evolutionary mechanisms. Machine learning and artificial intelligence are prime examples of the need for efficient technology for surveillance and censorship purposes.

Verhelst et al. (p 2975, 2020) claim “rapid advancements in machine learning techniques allow mass surveillance to be applied on larger scales and utilize more and more personal data.” Rephrased, society pushed the innovation of machine learning technologies that in turn have a greater social impact. Falling directly in line with the “automatic” theme of Kershner’s attitudes, this trend can be extended to the US, where the NSA employed such technologies within its PRISM program—the very program responsible for wide-scale wiretapping. In China, we see the “automatic” attitude by Xi Jinping’s government that “hopes to achieve full video coverage of key public areas” where citizens can be identified by an “AI matching them to an ocean of personal data, including text communications” (Andersen, 2020, n.p.). Although Western governments (and media outlets) often portray China’s surveillance of its people as draconian, multiple nations exposed by Snowden—like the United Kingdom, Germany, Sweden, France, and The Netherlands—are not far off from their Chinese peers.

Also apparent is the “Skepticism” component of Techno-Attitudes. The cases of China and the United States have caused significant plain pessimism, or “Technophobia”—an attitude where technology is seen as bad for both human and nature. Technophobics use the given actions to prove that ML/AI has no role in the hands of governments. Many then point to “the curse of dimensionality,” which can roughly be defined as “as the number of features [in a machine learning dataset] increases, the performance, and accuracy of machine learning algorithms

degrades" (L'Heureux et al, 2017, p. 7780). Anderson (2020, p. 2978) explains this principle's connection to mass surveillance as the implication that "selecting more details per suspect can increase the accuracy of the algorithm, but entails a need for a much more extensive data set." That in turn would require even greater surveillance and data collection from a nation's citizens. For this reason, skeptics of ML/AI technologies consistently uphold the notion that such technologies are significantly detrimental to the personal privacy of mankind.

ANT can be applied to this the current technical landscape by analyzing the ever-developing relationship between new actors that are entering the world of ML/AI surveillance. In the past, such technologies were in development and possession of only academia and large technology company research groups. The actors around the technology changed again as the technology proliferated government hands. As nations compete with one another, blocs are formed. Yet again, the actors in the network were extended to include allies of technologically advanced nations. Anderson (2020, n.p.) claims China "is now the world's leading seller of AI-powered surveillance equipment."

More interesting is how the interactions between the network consisting of China and its allies. Anderson (2020, n.p.) quotes Michael Kratsios, the then Chief Technology Officer of the United States when he mentions, China utilizes "predatory lending to sell telecommunications equipment at a significant discount to developing countries, which then puts China in a position to control those networks and their data." The source gives the example of Chinese AI startup CloudWalk Technology—a company that set up surveillance networks for the Zimbabwe government in return for sending images of the citizens of Zimbabwe back to company headquarters. The images were used to tune CloudWalk algorithms to better identify colored faces. Therefore, the most threatening consequence of China involving other actors isn't the

actors themselves, but the interaction of control China has over its allies. For this reason, security specialists assume that the new network governments utilizing AI for surveillance purposes pose a great risk to personal liberties and give an extensive amount of global power to China.

Video-based ML technology has long been regarded to be powerful for surveillance. Joshi et al. (2019, p. 239) place emphasis on "active surveillance" where cameras can detect suspicious behavior themselves. The technologies of ML and "computer vision have performed the tasks of extracting human actions from videos." These actions can then be used by national entities, like China's IJOP to further press on social control.

The final STS framework, engineering as experimentation, play a role in understanding the use of ML/AI by national governments. Yet again, there is little discernable difference in this aspect between both the United States and China. Many police departments in the US use new and experimental ML algorithms to aid with crime prevention. Verhelst et al. (2020, p. 2977) describe an example in New York City where an ML algorithm has been successful in predicting areas where car theft may be common. Other algorithms determine where to dispatch police patrols based on crime location data. This use of ML has been successful in its limited applications. However, this application is best explained as "engineering as experimentation" as data is collected from unknowing citizens, and tax-payer-paid funds are used to dispatch patrols to areas that may already be being over-policed. Feldstein (2019, n.p.) claims when "AI learning is used in policing," many studies have found them to "reinforce existing inequalities and produce or perpetuate discriminatory behavior." The source continues to explain that such crime-deterrence algorithms depend on data biased against minorities. This case illustrates a prime example of how AI applications, when deployed to the real world, are a form of experimentation that has significant societal pitfalls.

China's implementations of similar technologies also fall under the same "engineering as experimentation." Anderson (2020, n.p.) claims, China as being "an ideal setting for an experiment in total surveillance" because "Its population is extremely online." Of the over 1 billion mobile phones with sophisticated sensors, each can provide data points that "can be time-stamped and geo-tagged." This data collection is done in silence and out of view of the Chinese public. Behind government-sponsored technology companies, the experimentation relies on data from citizens that have no option but to give their data away.

After the analysis of both the United States and China in their use of ML/AI in surveillance and censorship, both nations somewhat perform the same actions. Although China has access to significantly greater information than the US, American companies and national governments attempt to use similar practices for their similar motives. Using ANT, Techno-Attitudes, and *engineering as experimentation* frameworks, we notice the same threats to privacy and personal liberties. Figure 3 compares the use of ML/AI technologies between the United States and China split by sociotechnical method.

	Actor-Network Theory	**Techno-Attitudes**	***Engineering as Experimentation***
China	Exporting AI technologies to allies but maintaining technological control.	Determinism: Using ML/AI for greater social control, which in turn allows for greater technological power.	Over extensive collection of data from its population. An estimated 1 billion devices are tapped with their owners unknowing.
United States		Automatic: NSA's PRISM program wiretapping citizens, readings emails, and instant messages.	NYC Police crime deterrence algorithms collected information from unknowing citizens to feed algorithms that were not fully tested.

Figure 3. Results Summary.
Table Portraying the results of China and the United States falling against the sociotechnical methods. (Created by Author)

One use of such technologies that preserve such liberties while being of utility to national governments is the use of only metadata for machine learning models. Metadata is defined as "data about data" (Verhelst et al. 2020, p.2976). For example, instead of reading emails and calls, models can use "the length and time of communication and the phone numbers or email addresses of those communicating but not what was written or said" (Verhelst et al. 2020, p.2976). The source then claims that machine learning algorithms can infer much more with the metadata. Although this use of machine learning preserves privacy, it will seldom be adopted by governments.

Examples of the NSA PRISM program and China's IJOP are key examples of organized overreach by nations. Both the US and China perform "engineering as experimentation" by using new technologies to collect data from unknowing citizens. This data is then used for algorithms that are not fully tested. In all, the dissection with the sociotechnical topics illustrates that the democraticness of a nation does not correlate with greater freedoms from ML/AI based surveillance.

IV: Conclusion

After the analysis of ML/AI applications for government uses of surveillance and censorship, a few previously unknown trends were found when STS frameworks were applied. Specifically, the frameworks of Actor-Network Theory, Techno-Attitudes, and "engineering as experimentation" showed that although nations may portray themselves to be nobler than their advisories when it comes to the use of ML/AI in censorship and surveillance, most nations with such technologies have systematically violated personal privacies and liberties.

The frameworks of ANT demonstrated that although key frontrunners of the technology are sharing the technology with other nations, it often is conditional on technologically advanced

nations gaining greater control over the smaller nation. The introduction of unknowing nations, as well as control by nations like China, changes the Actor-Network of the technologies significantly. An analysis of Techno-Attitudes by the public illustrates significant skepticism as well as some determinism of the use of ML/AI by the national governments of China and the US. Technological determinism has allowed China to use social control to push technology, as well as use technology to have greater social control.

If machine learning and artificial intelligence-based surveillance and censorship go unchecked, the world would progress into being a constant surveillance state—thereby making the panopticon analogy stronger. Ordinary law-abiding citizens would become prisoners to the very governments tasked to protect them. China's Xinjiang region shows the greatest extent of the panopticon effect with the mass extent of government control and surveillance. This paper's goal was to offer one step in the right direction with a lesson from sociotechnical analyses to formulate better strategies for responsible ML/AI use.

Works Cited

Aminuddin, M. A., Fitri, Z., Kaur, M., & Singh, D. (2018). A survey on Tor encrypted traffic monitoring. *International Journal of Advanced Computer Science and Applications*, *9*(8). https://doi.org/10.14569/ijacsa.2018.090815

Andersen, R. (2020, July 30). The Panopticon is already here. The Atlantic. Retrieved March 16, 2022, from https://www.theatlantic.com/magazine/archive/2020/09/china-ai-surveillance/614197/

Feldstein, S. (2019, January 22). *We need to get smart about how governments use AI*. Carnegie Endowment for International Peace. Retrieved March 16, 2022, from https://carnegieendowment.org/2019/01/22/we-need-to-get-smart-about-how-governments-use-ai-pub-78179

Gellman, B., & Adler-Bell, S. (2021, April 17). *The Disparate Impact of Surveillance*. The Century Foundation. Retrieved March 23, 2022, from https://tcf.org/content/report/disparate-impact-surveillance/?session=1

Goodin, D. (2014, January 21). *Scientists detect "spoiled onions" trying to sabotage Tor Privacy Network*. Ars Technica. Retrieved November 1, 2021, from https://arstechnica.com/information-technology/2014/01/scientists-detect-spoiled-onions-trying-to-sabotage-tor-privacy-network/.

Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. *Electronic Markets*. https://doi.org/10.1007/s12525-021-00475-2

Joshi, A., Jagdale, N., Gandhi, R., & Chaudhari, S. (2019). Smart surveillance system for detection of suspicious behaviour using machine learning. *Advances in Intelligent Systems and Computing*, 239–248. https://doi.org/10.1007/978-3-030-30465-2_27

Kerschner, C., & Ehlers, M.-H. (2016). A framework of attitudes towards technology in theory and Practice. *Ecological Economics*, *126*, 139–151. https://doi.org/10.1016/j.ecolecon.2016.02.010

Larrondo, M. E., & Grandi, N. M. (2021). Inteligencia artificial, Algoritmos y Libertad de Expresión. *Universitas*, (34), 177–194. https://doi.org/10.17163/uni.n34.2021.08

Latour, B. (1992) 'Where are the missing masses? The sociology of a few mundane artifacts', in Bijker, W. E. and Law, J. (eds) *Shaping Technology/Building Society: Studies in Sociotechnical Change*, Cambridge, MA, MIT Press, pp. 225-58.

Leibold, J. (2019). Surveillance in China's Xinjiang region: Ethnic sorting, coercion, and inducement. *Journal of Contemporary China*, *29*(121), 46–60. https://doi.org/10.1080/10670564.2019.1621529

L'Heureux, A., Grolinger, K., Elyamany, H. F., & Capretz, M. A. (2017). Machine learning with big data: Challenges and approaches. *IEEE Access*, *5*, 7776–7797. https://doi.org/10.1109/access.2017.2696365

Llansó, E. J. (2020). No amount of "AI" in content moderation will solve filtering's prior-restraint problem. *Big Data & Society*, *7*(1), 205395172092068. https://doi.org/10.1177/2053951720920686

Martin, M. W., & Schinzinger, R. (1997). Engineering as Social Experimentation. In *Ethics in engineering Mike W. Martin, Roland Schinzinger*. essay, McGraw-Hill.

McCahill, M. (2007). US and them – the social impact of 'new surveillance' technologies. Criminal Justice Matters, 68(1), 14–15. https://doi.org/10.1080/09627250708553275

Petit, P. (2019). 'everywhere surveillance': Global surveillance regimes as techno-securitization. *Science as Culture, 29*(1), 30–56. https://doi.org/10.1080/09505431.2019.1586866

Preece, A., Harborne, D., Raghavendra, R., Tomsett, R., & Braines, D. (2018). Provisioning robust and interpretable AI/ML-based service bundles. *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*. https://doi.org/10.1109/milcom.2018.8599838

Stoycheff, E., Liu, J., Xu, K., & Wibowo, K. (2018). Privacy and the panopticon: Online mass surveillance's deterrence and Chilling effects. *New Media & Society, 21*(3), 602–619. https://doi.org/10.1177/1461444818801317

Verhelst, H. M., Stannat, A. W., & Mecacci, G. (2020). Machine learning against terrorism: How big data collection and analysis influences the privacy-security dilemma. *Science and Engineering Ethics, 26*(6), 2975–2984. https://doi.org/10.1007/s11948-020-00254-w