Celeste Brevard

Government and COVID-19

Surveillance Technology and National Crises

New York University

August 6, 2020

The Patriot Act that was passed into law after the September 11th attacks made it easier for the government to use surveillance technology on citizens regardless of whether they were suspected of suspicious or illicit activities. This trend in surveillance technology can also be seen in China with its utilization of CCT cameras and other biometric surveillance technology. Much like the terror attacks in the United States, this trend was justified by the need to "assimilate" and monitor the Uyghur population associated with terrorist attacks in the region. Due to the fear caused by these attacks most citizens in each country did not have an issue with this lapse in the protection of their privacy. While the United States and China have different governing styles- the United States being a democracy and China an authoritarian regime-the use of these technologies doesn't look that different. With COVID-19 spreading across the globe and conversations around contact tracing through phone applications and other surveillance technology such as location data or creating "immunity passports" as a requirement to travel or obtain employment, will the public be accepting of relinquishing more of their freedoms to stop the spread of this virus? Surveillance technology is prominent in China and is increasing in the United States rapidly. This technology does have its benefits. It allows agencies such as the local police, the F.B.I, and Department of Justice to find potential suspects faster and could potentially help eliminate the global pandemic by centralizing the process of contact tracing. However, depending on where the technology is developed and who is programming it, these technologies have different built-in biases. As COVID-19 offers governments another major event generating mass public fear, it could offer an opportunity to sway public opinion on the wide-spread use of this technology. This paper will examine historical increases in the use of technology by the United States and China after terrorist attacks and address the subsequent impact on civil liberties in these regions. By comparing these countries of various political structures and their

usage of surveillance technology, this essay will address what depletion of freedoms may be associated with this increased use of technology in the name of public safety and its effect on the disenfranchised. While research has been done on surveillance technology and inequality, it has not been applied to its potential use in the current pandemic nor has its use in China and the United States been evaluated in this context. These two countries were chosen because of their prominent positions on the world stage, differing rules of law, and the fact that they are two of the largest developers of surveillance technology globally. Thus, should this technology be adopted, it will most likely have origins in one of these countries. Therefore, researching the implications of surveillance technology on the rights of civilians in times of turmoil is critical to understanding how a pandemic can be used to further the use of this technology and the societal impacts.

Before discovering the impact of surveillance technology on society, an introduction must be made into what surveillance technology entails. Surveillance technology changes as new technologies are developed. It can include bulk data interception, ICT monitoring, geo-location or remote sensing, data collection on the network of the internet of things, or biometrics.[1] The majority of this paper will focus on biometric surveillance technology. Specifically, facial recognition, as this technology is the newest in the field and has been adopted by both the United States and China. While the technology itself is important, the data gathered from technology and its uses must also be given attention. Shoshana Zuboff addresses this in her book, *The Age of Surveillance Capitalism*. She tasks the audience with realizing the full impacts of this technology cannot be entirely comprehended as this is not something that society has dealt with in the past.

[1] Ünver, "Politics of Digital Surveillance," 7.

Zuboff utilizes the term "instrumentarian power" to describe how she foresees surveillance technology will be turned into a capitalistic force, in which autonomy and democracy are traded for information about a consumer. She argues this will be used not only for advertisements for retail items, insurance, and financing, but to create behavioral underwriting that can impact how individuals vote and act.[2] The beginning stages of this can be witnessed when turning on a computer to research a new product then finding the advertisements being shown on a different device, or social media service have shifted to match the type of product that was being researched on another computer. While these small violations of behavior and interest have no dramatic consequences in most situations, Brexit-which will not be discussed in detail here-was in part the result of Cambridge Analytica's exploitation of instrumentarian power. The targeted advertisements distributed to very specific groups of people, whether containing accurate information or not about what Brexit would do for Great Britain, lead to the removal of an entire nation from an international organization by preying on individual behaviors and beliefs not previously accessible by organizations. This is relevant to surveillance technology as knowing where people are, who they associate with, and what products they buy, can not only allow those with the information to behavioral underwrite but can lead to the targeting of minority groups or people with beliefs different from those in power who control the technology.

The United States is a democracy. A place in which the people are supposed to have the ability to alter practices, leaders, and institutions which no longer serve them. Therefore, shouldn't surveillance technology be something the people are well versed on and have control

---

[2] Zuboff, *The age of surveillance capitalism*.

over? Unfortunately, this technology is not something that is being created merely as a result of progression or convenience. It is also born out of something more pressing, security. Thus, the legal and political process of informing the public is often withheld in the name of public safety. As Timothy Snyder states in *On Tyranny: Twenty Lessons from the Twentieth Century*, "Modern tyranny is terror management." In his book, he describes the Reichstag fire in Germany and attributes it to the moment in which Hitler's government was able to come to power through democratic means by using fear as a unifier. He attributes Putin's rise in Russia to the same type of alarm management against terrorist attacks.[3] While some may think these stories represent mere correlations that could only impact those abroad of a different government or different time, the September 11th attacks and the resulting domestic and international surveillance offer a different narrative.

The Patriot Act that was passed 6 weeks after the terrorist attacks on U.S soil offers a historical representation of how surveillance technology can be rapidly applied to a situation and have lasting impacts on civilian liberties. The Patriot Act was adopted on October 26, 2001. This granted agencies such as the F.B.I and the Department of Justice the ability to search property and residences without prior notification, pursue individuals such as computer hackers without warrants and gave them access to information such as medical and library records as well as private banking. The act itself covers a broad range of surveillance and is 300 pages in length. Due to its massive nature and the pressure to act after 9/11 as swiftly as possible, it was not read in its entirety by many politicians before it was passed. The main relevance to this topic is the portion that governs surveillance through the internet. Due to the decentralized nature of terrorist organizations, some argue that monitoring internet activity is essential to detecting and

[3] Snyder, *On Tyranny*, 103-107.

preventing future incidents. The nature of the internet, however, does not allow for the information of a potential terrorist and a civilian to be so easily deciphered. The sheer size of information collection is evidence of this. For example, in 2002, 440,606 terabytes of emails alone were collected. That would be approximately 7,344 trillion copies of this paper alone. With this, the erosion of the Fourth Amendment and Title III that were created to ensure civilians were guaranteed a certain amount of privacy without due cause began slipping away.[4]

Efforts to curb these surveillance practices have only taken place in the last 5 years. The USA Freedom Act did not pass until June 2015, 14 years after the terrorist attacks that quelled the masses into submission of their privacy for the common good. With its passing President Obama promised the act would give back some of the civil liberties the Patriot Act had taken away by limiting practices such as the bulk collection of data. Yet, as late as June of 2018 it was found that the National Security Agency experienced "technical irregularities" which lead to the collection of "call detail records" or CDRs it was not legally permitted to collect. However, the NSA stated it could not separate the legal information from that illegally obtained.[5] This comes 5 years after the June 2013 revelation by Snowden of the impact of Section 215 of the Patriot Act on mass phone logging which proved to be illegal in the first place.[6] With the advancement of technology and the development of encrypted chats, the likelihood of terrorists communicating over the phone and being intercepted by the NSA's CDR program is limited. Furthermore, after being reviewed by the Privacy and Civil Liberties Oversight Board, both Section 215 of the Patriot Act and Section 702 of the Foreign Intelligence Surveillance Act which allows the international communication of citizens to be monitored for "foreign intelligence", were only

[4] McAdams, "Internet Surveillance after September 11."
[5] Franklin "Fulfilling the Promise of the USA Freedom Act."
[6] Friedersdorf, "The Vindication of Edward Snowden."

attributed to identifying one terrorist suspect. Although the Safeguarding Americans' Private Records Act of 2020 still has some privacy loopholes, it is aimed at addressing most of the Fourth Amendment concerns presented by the laws enabled by the Patriot Act that were not addressed by the USA Freedom Act. While it was introduced to the house in January of this year it has yet to be passed. The Patriot Act and the subsequent legislation aimed at curbing its reach have both supporters that deem these practices necessary for national security and its naysayers who condone its reduction of privacy protections. Whether or not you agree with Snyder's statement, "People who assure you that you can only gain security at the price of liberty usually want to deny you both"[7], the point of this historical analysis is to illustrate the speed at which surveillance technology was adopted in the United States at the federal level after September 11th, the breadth in terms of information collection, the inaccuracies, and the difficulty in altering these adoptions over time.

The above civil rights concerns only refer to surveillance technology that has been passed into law in the United States. However, private companies' use of this new technology is surpassing legislation and a rapid rate. Clearview AI is a technology company that operated secretly until this year when the New York Times released a story about their operation. Mr. Thon-That, the founder, began in 2016 by "scraping" the internet for photos. All sites, despite their terms and conditions, were targeted. Social media sites such as Facebook, YouTube, Twitter, Instagram, and even the financial site Venmo were scoured for images that could be used in their new facial recognition software. Educational and employment sites were also used. By 2017 they had a range of ideas for how the product could be used and who to sell it to. Among them, Paul Nehlen, a Republican who describes himself as "pro-white" suggested it be

[7] Snyder, *On Tyranny*, 103-107.

used for “extreme opposition research.” While the company did not choose to pursue this option according to the article, they rebranded and began selling their new tool to the police. The Indiana State police became Clearview AI’s first customer. Using their product, the department was able to solve a case that involved a shooting and a man not in government databases within 20 minutes. The officers were able to run a video a bystander took through the system and find out who the perpetrator was through another video he was tagged in. This was possible because the database Clearview AI boasts consists of 3 billion subjects compared to the 411 million the F.B.I offers. Not only does this technology allow those searching the database to use personal photos that have been uploaded, but it also records images as obscure as the reflection of another person in someone else’s photo putting them in the system through images they may not even be aware are in the cybersphere.[8]

The main issue with companies such as Clearview AI is that the technology has been adopted without oversight or testing and thus, has built in biases. The company states a match can occur 75% of the time. However, the National Institute of Standards and Technology has not yet tested how effective the technology is. Furthermore, Clare Garve of Georgetown University’s research center on Privacy and Technology says the larger the database the more likely a doppelgänger effect occurs.[9] The National Institute of Standards and Technology did come out with a study in December of 2019, one month before the release of the New York Times article and in it, there is an abundance of research that proves artificial intelligence is a program created by humans and therefore, contains the biases of the database it uses and the programmers who create them. While their research only includes government-issued identification such as those

[8] Hill, “The Secretive Company That Might End Privacy as We Know It.”
[9] Ibid.

attained from DMV records or mug shots, their research details the accuracy of this technology on people of different country origins, age, sex, and race. They found false positives, or "incorrect associations of two subjects" were "between 2 and 5 times higher in women than men." Their research also showed false positives were the worst among American Indians, African Americans, and Asian populations. In their report, they admit the potential consequences of this imperfection on society. It reads, "In identification applications such as visa or passport fraud detection, or surveillance, a false positive match to another individual could lead to a false accusation, detention or deportation." They admit that algorithms developed in China produced low false positives for East Asian faces but were worse at identifying Caucasian faces. As East European individuals were among the lowest false positives for American facial recognition technology, they reiterated findings from their 2011 study that found "the location of the developer as a proxy for the race demographics of the data they used in training – matters…and is potentially important to the reduction of demographic differentials due to race and national origin." [10] It is not clear whether it is simply the demographic of the location providing the dataset that is the main proponent of the biases in the system or a combination of data and those creating the algorithms. The AI Now Institute of New York University which researches the social repercussions of AI noted in their report from 2019 entitled, "Discriminating Systems: Gender, Race, and Power in AI" that 80% of AI professors were men while in comparison only 18% of authors leading AI conferences were women. The trend continues with only 10% of AI Researchers at Facebook and 10% at Google being women. The statistics get worse when it comes to black employees. Only 2.5% of Google's workforce is black and only 4% of Facebook

[10] Grother, "Face recognition vendor test part 3," 2-8.

and Microsoft's staff are black workers.[11] Therefore, it is not surprising that the research that has been conducted in the field of commercial facial recognition, such as the study conducted by Joy Buolamwini from MIT and Timnit Gebru from Microsoft, produced similar findings to that of the NIST report. Their research used API bundles by Microsoft, IBM, and Face ++. Specifically, Microsoft's Cognitive Services API and IBM's Watson Visual Recognition API due to the large investments made by both companies in this technology. They created a database called the Pilot Parliaments Benchmark using the Fitzpatrick scale, a classification system for human skin color using numerical values. In the study, they also found the results were more accurate on lighter male faces and worse on darker female faces.[12] These built-in biases show that artificial intelligence has human origins that can lead to misidentification and therefore, unnecessary suspicion and detention. This was the case for Robin Williams, a black man, who was detained in Michigan for over 30 hours after he was falsely matched with facial recognition software and arrested in front of his children.[13] The biases built into the system discussed do not begin to deal with the social implications of gender categorization on gender non-conforming or trans-individuals. While it is not clear if the gender classification is built into the systems themselves or are simply used in the identification categorization process, each of the reports mentioned identifies potential issues within this categorization process in terms of gender association in addition to skin pigmentation. As the social implications of these programs become clearer, attempts are being made to stop their use without oversight. Companies whose data was scraped by Clearview AI without their consent have issued cease and desists. The ACLU has begun suing

[11] West, "Discriminating Systems: Gender, Race and Power in AI," 3.

[12] Buolamwini, "Gender shades: Intersectional accuracy disparities in commercial gender classification." 77-91

[13] ACLU. "Man Wrongfully Arrested."

the company under various state privacy laws such as the Biometric Information Privacy Act in Illinois.[14] However, these attempts take time and must be brought to the courts on a case by case basis. Furthermore, as will be discussed below, with the onset of COVID-19, the ability to instill laws protecting citizens may be deterred by the concern for public safety.

Before the ramifications of COVID-19 and its use of surveillance technology can be fully developed, the usage of this technology in China must also be investigated. In China, the private sector and the government are closely linked because of the communist authoritarian regime. It is expected that even foreign businesses adhere to government requests and restrictions placed on the populace or not be allowed to operate in China. Google restricting its services and filtering out content not allowed by the Chinese government is a prominent example of these policies as is the NBA being threatened after the Rockets' general manager tweeted in favor of Hong Kong civil rights.[15] Thus, the development of surveillance technology in China by private companies has been inextricably linked to the usage by the government in creating a surveillance state. Facial recognition technology has been combined with approximately 200 million cameras placed throughout China.[16] Facial recognition allows people into their apartments, is the main software behind "beautifying" phone applications, is a tool used by banks and ATMs, and in the "smile to pay" system set up at Kentucky Fried Chicken. This system is being developed within China and with the help of people from America. Graduate students as well as Microsoft and Google ex-employees eager to work in this emerging field despite its social implications contribute to the development of this technology in China. This plan called "Xue Liang" or "Sharp Eyes" is based on the Mao Zedong system of civil reporting but on a massive automated

[14] ACLU. "ACLU Sues Clearview AI."
[15] Rosenberger, "Making Cyberspace Safe for Democracy," 149.
[16] Feng, "How China Is Using Facial Recognition Technology."

scale. Eventually, the program will be used as a "social credit system" in which the activities of citizens are monitored, and they are awarded, or deducted points based on how well these activities align with the communist parties' priorities. This will be used to determine who qualifies for loans, employment, and even to predict crime.[17] In a hearing hosted by the House of Representatives subcommittee on Asia the Pacific and Nonproliferation, the human rights implications of this technology were debated. Testimonies were given from the director of Human Rights Watch, a student from the Hong Kong protest, and a Uyghur American whose mother was placed in the "re-education" camps in China. During this event, members of the House condemned the "digital authoritarianism"[18] and the "Orwellian Surveillance State" [19] China was exporting through the Belt and Road Initiative. Images from the film the "Minority Report" come to mind as each article and testimony details what the House and its witnesses describe. Those with "extreme thoughts" such as the Hong Kong protesters and Uyghur ethnic minority members are clearly subjected to this surveillance disproportionately to their Han ethnic majority counterparts. The reasoning being state security as each of these groups are viewed as a threat to the Chinese way of life, either through violence, a difference of thought, or both. The Chinese system, although pulling from a larger pool of data, also yields false positives. Chinese companies claim to have better accuracy than the F.B.I because of their large dataset and while specific accuracy results are not available, experts caution that false positives are still inevitable. Some have even speculated based on the research conducted in the United States that the

[17] Deneyer, "China's Watchful Eye."

[18] H.R. Rep. No. Hearing Before The Subcommittee On Asia, The Pacific And Nonproliferation Of The Committee On Foreign Affairs House Of Representatives One Hundred Sixteenth Congress "Authoritarianism With Chinese Characteristics: Political And Religious Human Rights Challenges In China," 13.

[19] Ibid, 2.

technology in China could be less accurate when applied to minorities such as the Uyghur population due to the same type of algorithmic bias in the data set that is seen in the U.S.A. It is easy to categorize this behavior as something unique to this type of regime. However, the United States, as has been shown above, is willing to use these invasive technologies as well. As of 2016, the United States had around 62 million surveillance cameras and a higher per capita penetration rate than China.[20] The Black Lives Matter protesters in the United States have been monitored through social media accounts and facial recognition software by local police departments and the Department of Homeland Security much like the Hong Kong protesters are targeted.[21] Thus, the two largest creators of surveillance technology resemble one another more than those of us living in a democracy care to admit. As Rosenberger writes, in "Making Cyberspace Safe for Democracy", "The challenge for democracies is to thwart authoritarians without playing into their hands."[22] The United States must be careful not to deal with the development of this technology like an arms race by allowing capitalistic pursuits to become a synonym for authoritarian control.

COVID-19 offers a similar gateway for increased surveillance technology to permeate society as do the terrorist attacks witnessed both on September 11th and in those allegedly carried out by the Uyghur minority population. The world has not been the same since this pandemic has taken hold. Economies have been dramatically impacted worldwide not to mention the daily lives of everyone on the planet. Jobs have been lost, stores, restaurants, and other social gatherings have been limited, and global events like the Olympics canceled. Therefore, it is understandable that the world is looking to resolve this crisis as quickly as possible. Those

[20] Deneyer, "China's Watchful Eye."
[21] Funk, "How Domestic Spying Tools Undermine Racial Justice Protests."
[22] Rosenberger, "Making Cyberspace Safe for Democracy," 154.

planning containment and re-opening strategies are searching all the tools available to them to make this happen. The American Enterprise Institute recommends monitoring those who have contracted the virus with GPS systems or cell-phone applications and calls for the "need to harness the power of technology".[23] The CDC website only details the use of COVIDTracer 1.0, a fairly manual excel sheet used by contact tracers to input information about those infected.[24] As of July 15th of 2020, however, hospitals were told to no longer report to the CDC. They have now been told to report their COVID-19 numbers to federal contractors such as Teletracking Technology out of Pittsburgh or to states who will report to the federal government. This was done at the White House's behest. Discussions around having the National Guard assist hospitals with reporting have also been recently released.[25] These changes in data collection processes will alter the ability to oversee how the data is collected and who it is given to. Thus, the process may become penetrated by other technology companies. One such company is FaceFirst from Encino, California. They are proposing more technological solutions such as a "coronavirus-immunity-registry" or "immunity passports" that use facial recognition technology on a cell-phone application run by medical providers. They suggest this could be used when traveling or applying for a position to show those interested what type of tests a person has received, whether they have been near someone infected, and whether they have had the antibody test.[26] This technology amplifies the discrimination built into the existing systems which has already resulted in specific groups being more impacted by COVID-19. It ignores the ability of people to access this type of technology because of a lack of financial means and does not consider that since

[23] Gottlieb, "*National Coronavirus Response."*

[24] CDC, "COVIDTracer 1.0."

[25] Sun, "Trump Administration Recommends the National Guard As An Option To Help Hospitals Report Coronavirus Data."

[26] Brewster, "Facial Recognition Firms Pitch Covid-19 'Immunity Passports' For America."

some groups have been hit harder by the pandemic, should this system be put into place, they could also be barred from future opportunities based on the tests they were able to receive and/or the treatment they could afford. Thus, this type of technology could not only lead to less privacy but could reinforce negative social systems that impact the un-enfranchised.[27] The combination of increased use of surveillance technology and the emergence of a global pandemic is, therefore, a potential for disaster.

As the Washington Post's new slogan states, "Democracy Dies in Darkness". The purpose of this research is not to prove that surveillance technology should be eradicated. Although, Amazon and Microsoft have done what some have called for and banned the development of facial recognition technology sales to law enforcement for the time being.[28] It is, however, to caution as Timothy Snyder, Shoshana Zuboff, and the Washington Post have, that security and privacy are luxuries that can be eroded under the guise of national security, technological progress, and civilian protection unless their uses are made public. Attention must be paid to the use, oversight, and trajectory of this technology. The United States and China are appropriate proxies for the potential global impact of this technology because of their global influence politically and as two of the most prominent producers and users of this technology. China has already begun exporting their cyber intelligence tactics by buying news outlets abroad and exporting their surveillance technology to the French city Marseille through the company ZTE.[29] While it is clear this technology can make the solving of criminal cases faster and eliminate the need to carry keys or a wallet, the flaws in the system that have been detailed throughout this paper should serve as a call to action. Laws need to be passed in anticipation of

[27] Toh, " How Digital Contact Tracing for COVID-19 Could Worsen Inequality."
[28] Taulli, "Facial Recognition Bans: What Do They Mean For AI."
[29] Rosenberger, "Making Cyberspace Safe for Democracy," 152.

the use of this technology and not in response as it has been shown how integrated this technology can become and how difficult its limitation is even under a government that claims to put the rights of the people before the priorities of the state. The new laws passed in Washington state that protect civil liberties by requiring surveillance technology to be used for specific instances and not mass surveillance serve as a promising framework.[30] China has a more developed program and fewer privacy rights. Thus, it provides a look into how "instrumentarian power" described by Zuboff can be so easily harnessed by the state and exploited based on its priorities. While the United States has implemented some of the same practices as China, there are attempts to change its trajectory that can only succeed when both its potential and problems are given the attention and space to be debated and the people are given room to decide how much of their information they are willing to relinquish for security both personally and at the national level. Otherwise, "when democracies fail to present a clear alternative to their authoritarian counterparts, they fuel growing perceptions that digital technology being developed in the United States is no different from that being developed in China."[31] Thus, the government needs to find the balance between ensuring innovation is not left to an authoritarian regime, but should work with the private sector and civil society to ensure its democratic values remain at the forefront of its development.

[30] Smith, "Finally, progress on regulating facial recognition."
[31] Rosenberger, "Making Cyberspace Safe for Democracy," 155

Bibliography

ACLU. (2020, June 24). Man Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart. Retrieved July 13, 2020, from https://www.aclu.org/press-releases/man-wrongfully-arrested-because-face-recognition-cant-tell-black-people-apart

ACLU. (2020, May 28). ACLU Sues Clearview AI. Retrieved July 13, 2020, from https://www.aclu.org/press-releases/aclu-sues-clearview-ai

Brewster, T. (2020, May 20). Facial Recognition Firms Pitch Covid-19 'Immunity Passports' For America And Britain. Retrieved June 24, 2020, from https://www.forbes.com/sites/thomasbrewster/2020/05/20/facial-recognition-firms-pitch-covid-19-immunity-passports-for-america-and-britain/

CDC. (2020, June 16). COVIDTracer 1.0. Retrieved July 14, 2020, from https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/COVIDTracer.html

Deneyer, S. (2018, January 07). China's Watchful Eye. Retrieved June 30, 2020, from https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/

Franklin, S. B. (2019, March 28). Fulfilling the Promise of the USA Freedom Act: Time to Truly End Bulk Collection of Americans' Calling Records. Retrieved June 26, 2020, from https://www.justsecurity.org/63399/fulfilling-the-promise-of-the-usa-freedom-act-time-to-truly-end-bulk-collection-of-americans-calling-records/

Feng, E. (2019, December 16). How China Is Using Facial Recognition Technology. Retrieved June 30, 2020, from https://www.npr.org/2019/12/16/788597818/how-china-is-using-facial-recognition-technology

Funk, A. (2020, June 22). How Domestic Spying Tools Undermine Racial Justice Protests. Retrieved July 14, 2020, from https://freedomhouse.org/article/how-domestic-spying-tools-undermine-racial-justice-protests

Friedersdorf, C. (2015, May 11). A Federal Appeals Court Vindicates Edward Snowden's Leak of NSA Secrets. Retrieved July 24, 2020, from https://www.theatlantic.com/politics/archive/2015/05/the-vindication-of-edward-snowden/392741/

Gottlieb, S., Rivers, C., McClellan, M., Silvis, L., & Watson, C. (2020). *National Coronavirus Response: A ROAD MAP TO REOPENING* (pp. 1-11, Rep.). American Enterprise Institute. doi:10.2307/resrep24613.3

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face recognition vendor test part 3:. doi:10.6028/nist.ir.8280

Hill, K. (2020, January 18). The Secretive Company That Might End Privacy as We Know It. Retrieved July 13, 2020, from https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

H.R. rep. No. Hearing before the subcommittee on Asia, the pacific and nonproliferation of the committee on foreign affairs house of representatives one hundred sixteenth congress-authoritarianism with Chinese characteristics: political and religious human rights challenges in china (2019).

McAdams, A. (2005). Internet Surveillance after September 11: Is the United States Becoming Great Britain? *Comparative Politics, 37*(4), 479-498. doi:10.2307/20072905

Rosenberger, L. (2020). Making Cyberspace Safe for Democracy: The New Landscape of Information Competition. *Foreign Affairs, 99*(3), 146-159.

Smith, B. (2020, July 07). Finally, progress on regulating facial recognition. Retrieved July 24, 2020, from https://blogs.microsoft.com/on-the-issues/2020/03/31/washington-facial-recognition-legislation/

Snyder, T. (2017). *On Tyranny: Twenty lessons from the twentieth century*. New York, NY: Tim Duggan Books.

Sun, L. & Goldstein, A. (2020, July 15). Trump Administration Recommends the National Guard As An Option To Help Hospitals Report Coronavirus Data. Retrieved July 22, 2020, from https://www.washingtonpost.com/health/2020/07/13/trump-administration-recommend-national-guard-an-option-help-hospitals-report-covid-19-data/

Taulli, T. (2020, June 13). Facial Recognition Bans: What Do They Mean For AI (Artificial Intelligence)? Retrieved July 24, 2020, from https://www.forbes.com/sites/tomtaulli/2020/06/13/facial-recognition-bans-what-do-they-mean-for-ai-artificial-intelligence/

Toh, A., & Brown, D. (2020, July 14). How Digital Contact Tracing for COVID-19 Could Worsen Inequality. Retrieved July 14, 2020, from https://www.hrw.org/news/2020/06/04/how-digital-contact-tracing-covid-19-could-worsen-inequality

Ünver, H. (2018). Politics of Digital Surveillance, National Security and Privacy. *Centre for Economics and Foreign Policy Studies*. Retrieved June 23, 2020, from www.jstor.org/stable/resrep17009

West, S.M., Whittaker, M. and Crawford, K. (2019). Discriminating Systems: Gender, Race and Power in AI. *AI Now Institute*. Retrieved from: https://ainowinstitute.org/discriminatingsystems.html.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York, NY: PublicAffairs.