Barry Eom
Comp 116: Cybersecurity
Professor Ming Chow

Defense Against the Dark AIS

The Risks and Mitigation of Artificial Intelligence Surveillance

Abstract

China is a frontrunner in artificial intelligence surveillance technologies, but liberal democracies—USA, France, Israel, etc—are also major users of AI surveillance. Due to the security benefits of artificial intelligence surveillance technology, facial recognition artificial intelligence surveillance deployment is expected to grow year by year worldwide. However, the technological pitfalls of artificial intelligence surveillance can increase unwarranted risk and harm marginalized groups. Moreover, artificial intelligence surveillance is a threat to freedom and democracies all over the world due to its sheer power—and some are already seeing the repercussions of it. Although there are individual efforts to resist against the power of artificial intelligence surveillance, the only way to counteract is through accountability through transparency and international effort to regulate artificial intelligence surveillance.

Introduction

It is quite evident that artificial intelligence has been the centerpiece of conversation not just in the technology industry but also in every imaginable industry, and will continue to be the dominating trend for the next decade or so, as the benefits of artificial intelligence are indisputable. But in the age where smarter and more intelligent technology is ingrained in the lives of many, governments have started to leverage AI for surveillance. Government entities can monitor every move of anyone in their own jurisdiction, which can fundamentally strip away the freedom of existing. Although the discussion of the lawful and ethical usage of AI

surveillance is warranted, this paper focuses on what one can do on an individual level to mitigate the threats of artificial intelligence surveillance.

To the Community

Governments and institutions around the world are incorporating artificial intelligence surveillance for the sake of security and safety, which to an extent is true; however, our freedom and democracy around the world is being jeopardized due to facial recognition artificial intelligence systems, as it grants significant power to governments utilizing the technology with no transparency. Without any awareness and immediate action by the people around the globe, artificial intelligence surveillance is a perfect tool for totalitarianism and *Big Brother Government* warned to us by George Orwell.

Background Information

The benefits of artificial intelligence surveillance technology, from here on out referred to as "AIS", has led to AIS ubiquitous inclusion in systems ranging from handheld mobile devices to surveillance cameras. With the ability to accurately identify faces in an instant, AIS system's usefulness for surveillance camera is undeniable. First and foremost, AIS monitors events in real time in high quality, unlike CCTV footages which are lower in visual quality and are viewed only after incidents have occurred. More importantly, AIS is significantly more accurate, efficient and time saving compared to the human eye. Human attention dip below acceptable levels after 20 minutes of watching CCTV footage,[1] whereas AIS systems would be immune to this, while being able to process significantly greater amount of data; most recently, earlier in September 2019, China unveiled 500 megapixel camera four times more accurate than the human with capabilities to identify every

[1] Reno, Janet, and Raymond Fisher. "The Appropriate and Effective Use of Security Technology in US Schools." *National Criminal Justice Reference Service.*

face in a crowd of "tens of thousands".[2] Beyond AIS systems, there are new technologies that can pre-detect potential violent acts using behavioral indicators through the observation of physical movement, personal demeanor, and other behavioral indicators[3] with PredPol (predpol.com) being a frontrunner in this space.[4] In terms of security for the safety of the masses, AIS is an appealing choice with significantly more utility than other alternatives.

However, the risks and dangers of AIS are alarming; AIS systems have fundamental technology flaws and more of a risk, leads to the loss of individual freedom and democracy. Starting from technological point of view, there are risks where AIS systems, despite its accuracy, causes false alarms that can result in dangerous confrontations. There is no denying that cases similar to Daniel Shaver, murdered in a hotel in 2016 due to an escalation of events despite no illicit wrongdoing on Shaver's part, is preventable from AIS. Moreover, AIS systems have been found to have significant bias in their data. Because training data is often heavily skewed towards white and male datapoints, there are inevitable racial shortcomings, leading to incidents where systems that predict that more black people are likely to re-offend and commit a crime[5] to darker skinned women being misidentified 35% more of the time.[6]

Going beyond technological flaws, AIS systems not only leads to misuse and abuse from those in power, but also compromises freedom on an individual level and democracy on a national and international scale. First, questionable use of surveillance is already underway with several incidents in 2019 Hong Kong

---

[2] Hayward, Freddie. "China Unveils 500 Megapixel Camera That Can Identify Every Face in a Crowd of Tens of Thousands." *The Telegraph*, Telegraph Media Group, 26 Sept. 2019
[3] Davis, Paul K., Walter L. Perry, Ryan Andrew Brown, Douglas Yeung, Parisa Roshan, and Phoenix Voorhies, Using Behavioral Indicators to Help Detect Potential Violent Acts: A Review of the Science Base, Santa Monica, Calif.: RAND Corporation, RR-215-NAVY, 2013. As of December 13, 2019
[4] Rieland, Randy. "Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?" *Smithsonian.com*, Smithsonian Institution, 5 Mar. 2018
[5] Angwin, Julia, et al. "Machine Bias." *ProPublica*, 9 Mar. 2019,
[6] Wingfield, Nick. "Amazon Pushes Facial Recognition to Police. Critics See Surveillance Risk." *The New York Times*, The New York Times, 22 May 2018

Protests where the anti-Chinese government protestors toppled surveillance cameras in fear of AIS and being marked by the Chinese government.[7] A system developed by Kosinski and Wang at Stanford University—a system that can recognize the sexuality of people[8]—can also lead to maleficent use of AIS. In states where homosexuality is criminalized, this system can be used to strip away the freedom of people based purely on their sexuality and physiognomy.

On top of the potential for misuse, AIS can lead to lack of trust between the government and its people. According to a report by American Civil Liberties Union (ACLU), people change and modify their behaviors if they know they are being watched.[9] Because of the ubiquity of AIS—with the number of surveillance cameras expected to exceed more than one billion—the essence of expressing and behaving freely is put into jeopardy. Currently, 75 of 176 countries and more than 50% of advanced democracies deploys artificial intelligence systems.[10] With AIS industry—valued at $9.6 billion—expected to continue its growth, a glimpse of what the world may look like is in Xinjiang, China, a province in Western China where the Uighar citizens behaviors are monitored nonstop.[11] Even worse, AIS has been utilized by the police to detain up to 1.8 million people.[12] With incredible power given to the government with AIS, the abuse of AIS systems that jeopardizes democracy is all too easy to foresee. Governments in autocratic and semi-autocratic countries are susceptible to abusing AIS systems, and countries with abysmal human rights track records are known for exploiting and abusing AIS systems.[13]

---

[7] Gleeson, Sean. "How Smart Are Hong Kong's Lampposts?" *AFP Fact Check*, 4 Sept. 2019
[8] "Advances in AI Are Used to Spot Signs of Sexuality." *The Economist*, The Economist Newspaper, 9 Sept. 2017
[9] "The Dawn of Robot Surveillance." *American Civil Liberties Union*, 13 June 2019
[10] Feldstein, Steven. "The Global Expansion of AI Surveillance." *Carnegie Endowment for International Peace*
[11] Buckley, Chris, and Paul Mozur. "How China Uses High-Tech Surveillance to Subdue Minorities." *The New York Times*, The New York Times, 22 May 2019
[12] Murgia, Madhumita. "Facial Recognition: How China Cornered the Surveillance Market." *Subscribe to Read | Financial Times*, Financial Times, 6 Dec. 2019
[13] Feldstein, Steven. "The Global Expansion of AI Surveillance."

Barry Eom
Comp 116: Cybersecurity
Professor Ming Chow

Action Items

As freedom is already compromised for some, severe action needs to be taken to mitigate the repercussions of AIS and prevent further compromising freedom and democracy. To do so, individual efforts have to be made to resist AIS. The simplest form is for individuals to make modification to their behaviors: evading AIS, seeking secure locations, and concealing one's identity. Additionally, some engineers and designers have also taken the matter to their own hands with three types of systems—software and wearables—developed to resistance of AIS. First, in a research published by Bose and Aarabi from University of Toronto, blocking facial recognition surveillance using adversarial attack was proposed, using another AI system to counter training efforts.[14] The University of Toronto system was able to reduce the identification accuracy from near 100% to between 0.5% and 5%. However, there are still ways to go for this system, as AI systems generally works differently. For wearables, a designer, Jip Van Leeuwen's anti AI Surveillance Mask , developed an anti AI surveillance mask that prevents AIS cameras to accurately capture the target's face (Image 1).[15] Similarly, HyperFace was developed by Hyphen Labs at MIT to confuse AIS systems from recognizing faces (Image 2).[16] However, as promising as these solutions sound, they are all temporary band-aid solutions to the ever evolving AIS systems deployed by nation states. New technologies can be adapted such that training images can be similar to the distortion or develop new methods of identification, e.g. gait recognition (walking form) or heartbeat recognition. As a result, there needs to be a collective legislative domestic and international effort to prevent AIS.

To do so, guidelines for all enterprises and companies must be enforced. ACLU recommends that "video analytics should not be used to collect identifiable

---

[14] Bose, Avishek Joey, and Parham Aarabi. "Adversarial attacks on face detectors using neural net based constrained optimization." 2018 IEEE 20th International Workshop on Multimedia Signal Processing (MMSP). IEEE, 2018.
[15] "Home." *Home*, www.jipvanleeuwenstein.nl/#m-masker.
[16] Harvey, Adam. "HyperFace." *Adam Harvey*, ahprojects.com/hyperface/.

information en masse or merely for seeking out 'suspicious' behavior" with transparency being the number one priority.[17] That being said, the only way to pragmatically enact considerable change is for the people to hold the government accountable. Most countries have already adopted AIS surveillance and others will undoubtedly follow suit—a question not of *if*, but *when*. As a result, the mitigation of repercussions of AIS depends on the quality of governance; speedy legislation that regulates the usage and transparency of AIS is the only practical solution to AIS's damages and impending threats. In the United States, calling local representatives and voting are realistic solutions that can ensure this accountability domestically; however, for authoritarian or corrupt nations, such is not an option. Therefore, on a universal scale, international agreement for refusal to purchase AIS without lack of clarity should be pushed by the United Nations.

Conclusion

The benefits of AIS are undeniable; however, the unregulated power that AIS grants to governments—even in the liberal democracies—are troubling with risks of false alarm and biases in training data. More crucial is that AI surveillance is already used as a tool to create a totalitarian state in Xinjiang, China—and others can easily follow suit. The only way to effectively regulate AIS are pushing for transparency for the government and guidelines for companies on an international scale—but this can only start with awareness and those who stand up for freedom and democracy.

[17] Chokshi, Niraj. "How Surveillance Cameras Could Be Weaponized With A.I." *The New York Times*, The New York Times, 13 June 2019

Barry Eom
Comp 116: Cybersecurity
Professor Ming Chow

Works Cited

"Advances in AI Are Used to Spot Signs of Sexuality." *The Economist*, The Economist Newspaper, 9 Sept. 2017, www.economist.com/science-and-technology/2017/09/09/advances-in-ai-are-used-to-spot-signs-of-sexuality.

Angwin, Julia, et al. "Machine Bias." *ProPublica*, 9 Mar. 2019, www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Bose, Avishek Joey, and Parham Aarabi. "Adversarial attacks on face detectors using neural net based constrained optimization." 2018 IEEE 20th International Workshop on Multimedia Signal Processing (MMSP). IEEE, 2018.

Buckley, Chris, and Paul Mozur. "How China Uses High-Tech Surveillance to Subdue Minorities." *The New York Times*, The New York Times, 22 May 2019, www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.

Chokshi, Niraj. "How Surveillance Cameras Could Be Weaponized With A.I." *The New York Times*, The New York Times, 13 June 2019, www.nytimes.com/2019/06/13/us/aclu-surveillance-artificial-intelligence.html

Davis, Paul K., Walter L. Perry, Ryan Andrew Brown, Douglas Yeung, Parisa Roshan, and Phoenix Voorhies, Using Behavioral Indicators to Help Detect Potential Violent Acts: A Review of the Science Base, Santa Monica, Calif.: RAND Corporation, RR-215-NAVY, 2013. As of December 13, 2019: https://www.rand.org/pubs/research_reports/RR215.html

"The Dawn of Robot Surveillance." *American Civil Liberties Union*, 13 June 2019, www.aclu.org/report/dawn-robot-surveillance.

Feldstein, Steven. "The Global Expansion of AI Surveillance." *Carnegie Endowment for International Peace*, carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

Barry Eom
Comp 116: Cybersecurity
Professor Ming Chow

Gleeson, Sean. “How Smart Are Hong Kong's Lampposts?” *AFP Fact Check*, 4 Sept. 2019, factcheck.afp.com/how-smart-are-hong-kongs-lampposts.

Harvey, Adam. “HyperFace.” *Adam Harvey*, ahprojects.com/hyperface/.

Hayward, Freddie. “China Unveils 500 Megapixel Camera That Can Identify Every Face in a Crowd of Tens of Thousands.” *The Telegraph*, Telegraph Media Group, 26 Sept. 2019, www.telegraph.co.uk/news/2019/09/26/china-unveils-500-megapixel-camera-can-identify-every-face-crowd/.

“Home.” *Home*, www.jipvanleeuwenstein.nl/#m-masker.

Murgia, Madhumita. “Facial Recognition: How China Cornered the Surveillance Market.” *Subscribe to Read | Financial Times*, Financial Times, 6 Dec. 2019, www.ft.com/content/6f1a8f48-1813-11ea-9ee4-11f260415385.

Reno, Janet, and Raymond Fisher. “The Appropriate and Effective Use of Security Technology in US Schools.” *National Criminal Justice Reference Service*, www.ncjrs.gov/school/178265.pdf.

Rieland, Randy. “Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?” *Smithsonian.com*, Smithsonian Institution, 5 Mar. 2018, www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337/.

Wingfield, Nick. “Amazon Pushes Facial Recognition to Police. Critics See Surveillance Risk.” *The New York Times*, The New York Times, 22 May 2018, www.nytimes.com/2018/05/22/technology/amazon-facial-recognition.html?module=inline.

Barry Eom
Comp 116: Cybersecurity
Professor Ming Chow

Images and Tables

Image 1

Image 2