Can CCTV Cameras and Artificial Intelligence Technology aid Crime Surveillance?

Jeff Zhang

American University

April 27, 2022

Can CCTV Cameras and Artificial Intelligence Technology aid Crime Surveillance?

Closed-circuit television cameras, also known as CCTV cameras, have been used for security monitoring for decades. CCTV cameras help law enforcement with criminal activity prevention, and in recent years new technology has expanded the capabilities of CCTV cameras. Artificial intelligence (AI) technology, namely facial recognition technology (FRT), is perhaps today's most implemented new technology in CCTV cameras. Facial recognition is powerful, and when used in conjunction with CCTV cameras, research suggests that they are both becoming more efficient in identifying people of interest than humans (Mileva and Burton, 2019). If the police are searching for a terrorist, CCTV cameras with facial recognition capabilities that are interconnected by networks and databases can support the automated detection of said terrorist, saving man-hours and resources. However, in the United States (US) and in other parts of the world, FRT is not extensively regulated. This lack of wide-scale governance creates several areas of concern. Proponents of regulating facial recognition in CCTV cameras argue that the technology infringes on people's civil rights, especially when someone is innocent of committing a crime. Does using CCTV cameras and FRT help prevent crime? Are the benefits of using CCTV cameras and FRT more worthwhile than their potential infringement on privacy rights? Through careful examination of their history, the research conducted in their area, the existing and proposed laws that govern them, and three case studies, CCTV cameras and FRT are mostly beneficial in protecting society. However, if we continue to use them extensively and expand their use in the future, CCTV cameras and FRT regulations must be increased by governments around the world. If governments fail to do so, there will be consequences for human rights, consent, and even authoritarianism.

CCTV cameras are widely used around the world. They work as a investigative tool for law enforcement, and they serve a large role in eliminating or reducing criminal activity in public spaces by simply making citizens conscious that they are being monitored

(Lippert and Wilkinson, 2010). There have been efforts to bring the public, law enforcement, and the media together to create protective communities, such as Crime Stoppers (Lippert and Wilkinson, 2010). Following the rise in the use of CCTV cameras in the 1990's in "open-street settings," Crime Stoppers began its educational awareness program on the effects of CCTV cameras by teaching the public what may constitute a "street crime" through advertisements (Lippert and Wilkinson, 2010). However, in their article on Crime Stoppers' work with CCTV cameras, Randy Lippert and Blair Wilkinson (2010) argue that Crime Stoppers' advertisements, while helpful, reveal detrimental effects of CCTV cameras. Lippert and Wilkinson (2010) noted that the advertisements showed "a remarkably narrow range of [criminal] acts," where other examples of harmful criminal acts that could've been equally or further persuasive were omitted. This implies the advertisements were detrimental to the public's imagination of crime and creates a narrative of CCTV surveillance failing to deter crime(Lippert and Wilkinson, 2010). Lippert and Wilkinson (2010) suggest that the improper use of CCTV cameras can distort the public's imagination of what crime is, and by limiting their knowledge of the capabilities of CCTV cameras, creates a bubble of false security.

Based on 40 years of systemic review on CCTV surveillance for crime prevention, Piza et al.'s (2019) research paper suggests that CCTV cameras are "associated with a significant and modest decrease in crime." Piza et al. (2019) also notes that an increase in CCTV camera usage is generally seen as a positive thing by both politicians and the public. By installing more CCTV cameras, politicians can express their concern about controlling crime to the public, and in return, the cameras help make the public feel safer. In fact, Piza et al. (2019) claims that "the increased prevalence of surveillance cameras in public places has led scholars to consider CCTV as a 'banal good' that has become part of everyday life, taken-for-granted by the public." In spite of a historical widespread positive outlook on CCTV cameras, Piza et al.'s (2019) research concludes that the rapid growth of CCTV cameras warrants new policy revision, and that it would "benefit from high-quality

evaluations of [the cameras'] outcomes and implementation."

As FRT advances, its use becomes more widely implemented in existing machinery. According to researchers Mila Mileva and Mike Burton (2019), visual search environments that contain human subjects are typically created based on tightly-controlled man-made criteria. While these experimental environments are great at presenting general principles of object recognition, Milva and Burton (2019) suggest that the results of experiments are difficult to translate over to more complex everyday visual searching. Mileva and Burton (2019) also explain that while there is a plethora of research done on object recognition on humans, there is actually very little known how these mechanics would perform in common everyday search tasks, but also in security critical tasks. For example, Milva and Burton (2019) describe a human experiment where test subjects were asked to "compare stills from the footage with high-quality targets in an eight-image line up or in a one-to-one matching task." The experiment's result showed humans could only accurately identify 29% of the targets in CCTV footage, and the error rate was high regardless of the number of distractors (Mileva and Burton, 2019). While their research was on human interaction with CCTV footage and not with AI interaction, Mileva and Burton's research shows how difficult it is for humans to correctly identify persons and objects of interest with CCTV cameras, let alone emerging technology such as FRT. The research also suggests that engineers would need to invest an enormous amount of resources into FRT development before it could potentially surpass human's identification skills.

Many countries in the world have laws on the use of CCTV cameras, and these laws encompass when CCTV cameras can be used in the context of privacy. According to the US Department of Justice (2020), law enforcement agencies may request to use video surveillance from the Department of Justice "when there is a constitutionally protected expectation of privacy requiring judicial authorization." This means that when there is an expectation of privacy for something that needs to be monitored by CCTV cameras, formal federal approval and sufficient reasoning is needed before law enforcement can install

CCTV cameras. However, the use of FRT is not federally regulated, and there are concerns about its potential effects when used with CCTV cameras for crime surveillance.

An example of effective American police usage of CCTV cameras for crime prevention can be recalled in Las Vegas, Nevada. The Las Vegas Metropolitan Police Department's (LVMPD) installation of CCTV cameras in a high-crime location within the city has been met with substantial community support, but it was only possible through careful research, planning, and implementation (Sousa and Madensen, 2016). During the initiative's planning stage, one of its biggest concerns was about privacy. In their article on LVMPD's CCTV surveillance system installation process, William Sousa and Tamara Madensen examined the CCTV camera's implications on privacy. They suggest that support and acceptance of CCTV cameras from citizens influences the effectiveness of camera operations (Sousa and Madensen, 2016). Sousa and Madensen (2016) explain that even when they were willing to make sacrifices to individual liberties in response to threats to national security or to personal security, citizens would argue the government could improperly use CCTV cameras to monitor citizens without due process. Some Las Vegas citizens were worried that law enforcement or even hackers could use the installed CCTV cameras "to clearly view and record over long distances and through windows of nearby buildings," rather than only monitoring public spaces (Sousa and Madensen, 2016). Sousa and Madensen (2016) say that, while there's little evidence that suggests crime cameras have been used illegally to monitor citizens or threaten individual rights, public resistance to cameras can develop if they are placed in areas that lack support for them. To address theses concerns, LVMPD adopted strategies focused on two areas: transparency in using the cameras and net-widening the crimes monitored by the cameras.

To increase transparency, LVMPD made sure their CCTV cameras were clearly visible to passersby as crime surveillance cameras by installing the cameras on a light pole with flashing lights and displaying the Department's emblem (Sousa and Madensen, 2016). During their CCTV camera system planning process, LVMPD routinely involved citizens in

decisions that could impact privacy concerns, which increased community support for using CCTV cameras (Sousa and Madensen, 2016). By ensuring their cameras were clearly visible to the public and getting the public involved in their installation process, LVMPD offered effective solutions to the public's concerns. For net-widening, LVMPD made sure their cameras were justly and efficiently used on all types of criminal activity. LVMPD assured the community that those who monitored the cameras would receive proper training and that patrol officers in the area would utilize appropriate levels of discretion for all types of crimes (Sousa and Madensen, 2016). Finally, LVMPD ensured the public that their CCTV cameras were not the only form of crime prevention in the area by establishing strategies to use the cameras in conjunction with other broader crime prevention initiatives (Sousa and Madensen, 2016). These other initiatives include officer patrolling, assistance from vice and narcotics units, and regular reporting on the initiatives (Sousa and Madensen, 2016). This strategy assured the Las Vegas public that crime prevention in the area was genuine, and the CCTV cameras were used to support more "on-hands" approaches to community safeguarding. LVMPD's CCTV surveillance system is a great example of properly using CCTV cameras as a way to keep the community safe, but it shows such a system requires careful planning and cooperation between authority and citizenry.

In recent years, FRT has become more ubiquitous in surveillance systems. US Congressional Research Service (CRS) analysts Kristin Finklea et al. (2020) point out issues with FRT. These issues include how accurate the technology is in identifying race and gender, how organizations should properly maintain their systems for collecting, storing, and securing data, and policies or standards governing law enforcement agencies' use of the technology (Finklea et al., 2020). These concerns are currently addressed by several proposed and enacted (albeit very few) city, state, and federal laws. Finklea et al. (2020) suggests that policymakers should consider three main points when creating legislation on law enforcement agencies' use of FRT:

1. Evaluate the accuracy of these systems is defined and assessed by law enforcement,

2. How to support or restrict the technology's use by federal, state, and local law enforcement—and potential implications, and

3. How to balance privacy and security concerns with supporting lawful criminal justice activities.

James Andrew Lewis, the Senior Vice President and Director of Strategic Technologies at the Center for Strategic and International Studies, argues that most people's current understanding of FRT is horribly misinformed. Lewis (2021) suggests that "FRT is improving rapidly, and any critique based on data from even a few years ago runs the risk of being entirely wrong." Lewis makes an important distinction between FRT and facial characterization, a distinction he believes will help mitigate misinformed criticism of FRT. For example, FRT, a biometric technology, compares two images and determines how likely one of the images is the same as the other, while facial characterization examines an image and tries to characterize it by gender, age, or race (Lewis, 2021). It seems that most people, including myself, may have some incorrect preconceptions about FRT. Lewis (2021) suggests people should be more informed on issues with FRT accuracy and bias before policymakers can create good laws.

Lewis (2021) explains FRT will continue to develop, regardless of public opinion, since its benefits for consumers and public safety are very great. Lewis' article is relevant in the discussion of the future of FRT in the US because it explains the areas FRT should be regulated in, the existing laws on its use, and what it means for society in the future. Calling them "guardrails," Lewis (2021) discusses the framework elements in developing FRT laws and regulations. They include permissible use, transparency, consent and authorization, data retention, autonomous use, redress and remedy, oversight and auditing, algorithmic review, and training data (Lewis, 2021). Lewis also explains the importance of assessing the guardrails' effects on privacy, which is particularly important in the case of FRT usage of CCTV cameras.

Despite Lewis' positive outlook in it, FRT has already caused controversy. In her article, Kashmir Hill discusses a recent story of how New Jersey's Woodbridge Police Department (WPD) misused FRT in a criminal case. In February 2019, WPD accused Nijeer Parks of shoplifting, attempted battery of a police officer with his car, and fleeing the crime scene (Hill, 2021). WPD supposedly matched Parks with the suspect's driver's license photo using FRT, and Parks was arrested and detained for 10 days in a corrections center, but he defended his innocence. It wasn't until November of the same year were his charges dropped due to lack of evidence. In her review of the case, Hill (2021) reports how WPD misused FRT in their investigation and the detrimental effects it would've had on Park had he been prosecuted.

Parks' lawyer suggested WPD used Clearview AI, a facial recognition app, in their investigation. The app uses billions of photos extracted from the public web, including social media such as Facebook and Instagram (Hill, 2021). The case's police report affirms Parks was matched due to similarities with a driver's license photo using Clearview AI. However, driver's license photos are stored in government databases, which Clearview AI does not have access to (Hill, 2021). It is unclear how WPD made the match between Parks and the license photo. Hill (2021) explains that "law enforcement often defends the use of FRT, despite its flaws," by saying it is used only as a means to support evidence and not to directly lead to an arrest. But in Parks' case, Hill suggests WPD directly used FRT as a warrant for Parks' arrest, even when their evidence was misconstrued or flawed. Also, because he had previously committed two felonies, had he been (wrongfully) convicted for a third felony in this case, Parks would risk a long prison sentence (Hill, 2021). Even though Parks was innocent, WPD's ambiguous use of FRT to charge Parks for the crime has horrible long-term repercussions. Parks remarked he felt "afraid" of his situation, and because of it he felt pressured to accept the prosecutor's plea deal (Hill, 2021).

Parks' case was not the first time bad facial recognition resulted in the arrests of innocent Black men. In Detroit, "two other Black men were also arrested for crimes they

did not commit based on bad facial recognition matches" (Hill, 2021). Hill (2021) supports these two instances with a 2019 national study of over 100 facial recognition algorithms, which found that the algorithms did not work as well on Black and Asian faces. Nathan Free Wessler, an attorney with the American Civil Liberties Union, believes law enforcement should stop using FRT since the Parks and Detroit cases show the technology "disproportionately harms the Black community" (Hill, 2021). Parks' case also caught the attention of New Jersey's attorney General, Gurbir S. Grewal, who put a temporary ban on using Clearview AI by the police and announced an investigation into it and those like it (Hill, 2021). Grewal's office revealed New Jersey was actually still evaluating the use of FRT in criminal cases and the development of its governing policy was ongoing (Hill, 2021).

Parks' case, Wessler's judgement, and Grewal's call to action all suggest that using FRT with CCTV cameras in crime prevention is too early to be effective. WPD grossly misused FRT, and it seems they couldn't even properly explain how they used it to charge Parks. WPD's failure to properly use FRT could've given Parks consequences he did not deserve, and this clearly shows a need for FRT legislation that can prevent something like this from happening again.In fact, Grewal even says New Jersey's laws on FRT are premature. Furthermore, this story serves as a reminder to FRT designers that they should widen the scope of their algorithms so it would be less likely to misidentify Black individuals and other people of color.

Laws and usage of CCTV cameras and FRT exist elsewhere in the world as well. Like the US government, the United Kingdom (UK) government supports the use of CCTV cameras in public spaces. In the UK, "surveillance camera systems are deployed extensively, and these systems form part of a complex landscape of ownership, operation and accountability" (GOV.UK, 2021). When they are used appropriately, these systems become "valuable tools which contribute to public safety and security" (GOV.UK, 2021). The UK realizes there is a need for extensive laws and regulations for which the cameras are used, rather than the technology itself (GOV.UK, 2021). This distinction is important

for the moral uses of CCTV cameras, since it shows that not only are the privacy concerns of using CCTV addressed, but they are also enforced by law.

To achieve the most appropriate balance between public protection and individual human rights, the UK government suggests CCTV surveillance operators adopt a set of guiding principles (GOV.UK, 2021). The UK has an official set of 12 guiding principles. They are specifically designed "to establish a clear rationale for any overt surveillance camera deployment in public places and to run any such system effectively" that is also compliant with the law (GOV.UK, 2021). Principles relevant to our discussion of CCTV cameras and FRT include:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need,
2. The user of a surveillance camera system must take into account its effect and justification on individuals and their privacy,
3. There must be as much transparency in the use of a surveillance camera system, and
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used (GOV.UK, 2021).

There seems to be an expectation for a responsible sense of duty when operating CCTV cameras. The UK expects operators, whether they are law enforcement officials or citizens, to have a legitimate and transparent reason to use a CCTV camera, to make sure its use does not infringe on the privacy of others, and to responsibly collect and store its collected data.

In the UK, the reigns that bind FRT to law are more opaque. The UK government acknowledges the merits and risks of using biometric technology, such as FRT, in different contexts, and within those contexts FRT may be helpful or detrimental to society

(GOV.UK, 2020). Similar to the US, the UK also acknowledges the rising worldwide public and political concern for FRT, and likewise, it was not until recently that the UK officially began creating FRT laws. In their 2019 court case against the South Wales Police (SWP), the civil liberties group *Liberty took South Wales Police* (LSWP) declared SWP's use of FRT had breached several civil rights acts. The UK Supreme Court initially determined SWP's FRT usage was based on a clear and sufficient legal framework (GOV.UK, 2020). But, after LSWP was granted an appeal of the court's decision, the UK Court of Appeals overturned the original ruling, concluding that SWP "had [actually] breached privacy, data protection and equality regulations" (Reuters Staff, 2020). This court ruling is very important in how we should treat FRT and its uses in surveillance. While there may be a preconception that current laws are sufficient in controlling FRT, we need to realize that this is unlikely to be the case. In places where there are no landmark court cases in regards to the use of FRT surveillance, extra caution is needed.

As a response to the UK Court of Appeal's ruling, the UK government (2020) urges policymakers and civil society groups to seek answers on how to meaningfully involve the public in deciding whether FRT should be used, and what for. As of May 2020, the UK's Center for Data Ethics and Innovation (CDEI) is supporting policymakers with their research on FRT's impacts on society, and the CDEI expects law enforcement to be appropriately transparent about how they use this technology (GOV.UK, 2020).

In the city of Liverpool in Merseyside, England, we have another case where a city installed CCTV cameras in an area of high crime rates for crime prevention. In the 1990's, Liverpool underwent economic growth. In 1992, the city established the Liverpool City Center Partnership (LCCP), which operated towards maximizing the city's downtown center's potential as a regional center in the Merseyside county by enhancing its attractiveness to all those who use it (Coleman and Sim, 2000). LCCP's "place marketing" strategy aimed to positively promote aspects of the city's "quality of life," including safety and crime prevention, as a way to re-image the city as a safe place to do business (Coleman

and Sim, 2000). As part of their place marketing, LCCP conducted a survey that suggested potential city center visitors were "deterred by fear of car crime, litter, vagrants, and gangs of youths," in that order (Coleman and Sim, 2000). In fact, a majority of those surveyed preferred to visit enclosed malls containing CCTV and a with a visible security presence (Coleman and Sim, 2000). Supplemented with existing law enforcement data that Liverpool maintained one of the UK's highest recorded crime rates, LCCP's survey showed that the City of Liverpool needed to increase security in the city center open spaces (Coleman and Sim, 2000). This incentivized the city to construct their CCTV network.

From LCCP's survey, we can assume CCTV cameras help people enjoy leisure activities in a care-free public environment. But does this mean people would support having CCTV cameras monitor public spaces? Researchers Roy Coleman and Joe Sim suggest this is the case. They note that the city's local retailers felt that CCTV cameras were a necessity to flip the city's negative image as a "dangerous place" and in the need to counter the "horrendous losses" from shop theft (Coleman and Sim, 2000). Local business owners and the private sector alike supported the city's CCTV network proposal. Similar to the Las Vegas case study, Liverpool citizens could voice their concerns about the CCTV system in regards to privacy, consent, and authority to the city government. Coleman and Sim (2000) note the Liverpool government, public, and private sectors had regular meetings as one central group known as *Crime Alert*. The *Crime Alert* meetings established the public and private sector's voice as "constructor, organiser, permanent persuader and not just as simple orators" (Coleman and Sim, 2000). Upon the completion of the camera system, LCCP deemed the system was effective in targeting those who have been identified as problematic in the city center while simultaneously reconstructing Liverpool's image and economy (Coleman and Sim, 2000). In other words, Liverpool's CCTV camera system was a success. Plus, the CCTV camera system follows the aforementioned four UK guiding principles on CCTV use.

CCTV camera systems have generally provided a net positive in reducing crime and

increasing the public's sense of safety. However, it may not be the same case if the cameras had FRT capabilities, or were used in conjunction with FRT. After reviewing the Las Vegas, Liverpool, and WPD vs. Parks case studies, we see the effects of using CCTV cameras and FRT for crime prevention purposes. On one hand, we can tell CCTV cameras are effective when they are implemented with widespread public, private, and official support and communication. But on the other hand, CCTV cameras equipped with new technology can be abusively used without a clear due process. By analyzing them through the Act-Utilitarianism ethical framework, we will determine if the three case studies show if CCTV cameras and AI technology should be used for crime surveillance.

Act-Utilitarianism is the ethical theory that an action is morally right if its net effect over all affected beings is to produce the greatest good and happiness (Quinn, 2020). In the Las Vegas and Liverpool case studies, officials from both cities were aware that crime in certain city regions were causing disturbances to the local population, and they proposed constructing CCTV camera systems to help mitigate the situation. Not only were the public in favor of such a system, officials saw the work as an opportunity to positively show the government's care for the community or to help boost the city's economy. The citizens of Las Vegas and Liverpool shared concern over certain aspects of their city's CCTV camera system, but their city governments openly addressed them by offering reasonable solutions. The public and government share the benefits of their new CCTV camera systems. People were happy to see reduced crime and they felt safer in busy areas of their cities, and the government accomplished their job with near universal support and did so with community involvement. Of course, it would seem criminals would be the most unhappy individuals when the city constructs a CCTV monitoring system that deters them from reaping the benefits of breaking the law. From an Act-Utilitarianism point of view, the Las Vegas and Liverpool case studies show CCTV cameras are an effective tool in supporting a community's safety.

For the Woodbridge vs. Parks case study, FRT was incorrectly used to arrest a man

for a crime he did not commit. Parks was initially imprisoned for 10 days, and charges against him weren't dropped until 9 months later. He noted the fear and anxiety he felt during the ordeal, feelings that were likely shared by the two men from Detroit who were also falsely accused by FRT. WPD wasted resources and man-hours on an investigation without realizing their prime suspect was obviously innocent from the start, and their public image was tainted by their mishandling of the case. With these points in consideration, it seems Parks, the two men from Detroit, and WPD suffered a net loss from their court cases. From an Act-Utilitarianism point of view, it's advisable to avoid using FRT for crime prevention.

Under the right circumstances, CCTV cameras have the potential to leave a positive outcome in crime prevention. But when used in conjunction with immature technology, like FRT, CCTV cameras may easily be misused. The Parks case showed the dangers of FRT, even if the technology intends to work for the good of society. CCTV cameras and FRT are capable crime prevention tools, and citizens are open to the idea of their city officials building security networks that incorporate such tools. But, these networks can only be successful when officials are transparent with the construction process and welcome the community to voice their needs and concerns. Laws for CCTV use spans back decades, and CCTV cameras are used around the world, meaning they are an established instrument of security. But for FRT, local, state, and federal governments should be wary of its consequential implications. There is a critical need to expand FRT regulations before governments hastily incorporate the technology into their criminal justice systems.

References

Coleman, R., & Sim, J. (2000). You'll never walk alone: Cctv surveillance, order and neo-liberal rule in liverpool city centre. *The British Journal of Sociology*, *51*(4), 623–639. https://doi.org/10.1080/00071310020015299

Finklea, K., Harris, L. A., Kolker, A. F., & Jr., J. F. S. (2020). Federal law enforcement use of facial recognition technology. *Congressional Research Service*. https://sgp.fas.org/crs/misc/R46586.pdf

GOV.UK. (2020). *Snapshot paper - facial recognition technology* (tech. rep.). The Government of the United Kingdom. https://www.gov.uk/government/publications/cdei-publishes-briefing-paper-on-facial-recognition-technology/snapshot-paper-facial-recognition-technology

GOV.UK. (2021). *Amended surveillance camera code of practice* (tech. rep.). The Government of the United Kingdom. https://www.gov.uk/government/publications/update-to-surveillance-camera-code/amended-surveillance-camera-code-of-practice-accessible-version

Hill, K. (2021). Another arrest, and jail time, due to a bad facial recognition match. *The New York Times*. https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html

Lewis, J. A. (2021). Facial recognition technology: Responsible use principles and the legislative landscape. *Center for Strategic and International Studies*. https://www.csis.org/analysis/facial-recognition-technology-responsible-use-principles-and-legislative-landscape

Lippert, R., & Wilkinson, B. (2010). Capturing crime, criminals and the public's imagination: Assembling crime stoppers and cctv surveillance. *Crime Media Culture*, *6*(2), 131–152. https://doi.org/10.1177/1741659010369950

Mileva, M., & Burton, M. A. (2019). Face search in cctv surveillance. *Congnitive Research: Principles and Implications*, *4*(1), 1–21. https://doi.org/0.1186/s41235-019-0193-0

Quinn, M. J. (2020). Ethics for the information age. *Pearson Education, Inc.*

Reuters Staff. (2020). Landmark uk court ruling finds police use of facial recognition unlawful. *Reuters*. https://www.reuters.com/article/us-britain-tech-privacy/landmark-uk-court-ruling-finds-police-use-of-facial-recognition-unlawful-idUSKCN2572B8

Sousa, W. H., & Madensen, T. D. (2016). Citizen acceptance of police interventions: An example of cctv surveillance in las vegas, nevada. *Criminal Justice Studies*, *29*(1), 40–59. https://doi.org/10.1080/1478601X.2015.1088230