Esper “Enhance”

From one scene, we have a number of possible parallels to 21st century privacy and related concerns. The scene in question features Blade Runner – Rick Deckard deciding to examine more closely a photograph confiscated from a replicants (Leon) hotel room. As well as examining by eye, he places the photograph into an Esper machine which performs further analysis. The Blade Runner press key from the 1982 release describes an Esper as “A high-density computer with very powerful three-dimensional resolution capacity. The police cars and Deckard’s apartment contain small models which can be channelled into the large one at police headquarters” [1].

[1] <http://www.brmovie.com/FAQs/BR_FAQ_Terminology.htm>. Accessed 29-11-2020

This scene brings about questions around modern day technology such as CCTV (Closed Circuit Television) or other image capture, and how pervasive this is. The fact that the movie shows access from a home and mobile device indicates that such analysis is freely available.

In today’s society with 4-5.9 CCTV cameras in the UK - 2015 estimate by BSIA (British Security Industry Association) [2].

“The potential value of public surveillance technology was well demonstrated all the way back in April, 2013 when investigators identified the two suspects in the [Boston Marathon bombing](https://www.ifsecglobal.com/video-surveillance/london-2012-boston-marathon-securing-large-scale-events/) after sifting through video images captured by the city’s cameras.

The Boston bombers were apprehended quickly due to surveillance cameras. While there is no dispute over how well the public cameras worked on that day, many lingering questions remain and will continue to drive debate for the foreseeable future.” [3]

Back in 2014, Delhi Metro CCTV footages were on YouTube and also at some questionable sites. Who owns responsibility for not misusing the data of public CCTV surveillance? In short – who decides and regulates?

[2] <https://www.bbc.co.uk/news/uk-30978995#:~:text=The%20UK%20has%20one%20of,between%204%2D5.9%20million%20cameras>. Accessed 29-11-2020

[3] <https://www.ifsecglobal.com/video-surveillance/role-cctv-cameras-public-privacy-protection/> Accessed 29-11-2020

## In favour of CCTV cameras

* We should have surveillance cameras in public places because they ensure public safety. Rarely will anyone attempt to harm you when they know their actions are being recorded on camera. Cameras keep you and your personal property safe.
* The police can identify criminals recorded with cameras. Through surveillance cameras, the police can both prevent crimes from happening and can quickly solve criminal cases with material evidence.
* In addition, surveillance cameras protect against property theft, and vandalism. It is very difficult to get away with stealing something if there are cameras filming you. Therefore, the thief will often get caught. Surveillance cameras will catch the thief before, or during the process of committing the crime.
* If no one is aware of the crime until after it has been committed, the surveillance footage is always a crucial piece of evidence during a police investigation. Surveillance cameras have, and will provide a solution to many crimes.
* Some people may say that we should not have surveillance cameras in public places. They claim that they invade privacy. The argument here, however, is why be out in public if you want privacy? Surveillance cameras are meant to keep you and other property safe, not to stalk you. Cameras are there not to invade a person’s privacy but to protect the public by deterring criminal activity and by providing material evidence when a crime has been caught on film.
* Criminals are less likely to commit crimes in the area if they know they’re going to be being filmed the whole time. Unscrupulous [activities like shoplifting hardly seem worth it when pitted against the possibility of going to jail.](https://www.ifsecglobal.com/uncategorized/ip-video-will-stamp-out-self-service-checkout-theft/)
* Having cameras in public places make people feel safe. If people know that there are cameras around them, they will most likely not do anything stupid. People feel safer in the knowledge that a potential mugger or attacker will be put-off by the presence of a camera.
* Cameras, through video analytics, now have the ability to zoom in to reveal someone’s identity which can be beneficial to crime prevention when used in the correct way. The criminal can be apprehended quickly. Especially in abduction cases a video would be a great way of tracking down a person quickly and maybe preventing a death!
* The growth of facial recognition and analytical software enables much greater predictive insights into criminal behaviour and more accurate reporting.

## ****The arguments against CCTV cameras****

* [It is an infringement on your civil liberties.](https://www.ifsecglobal.com/cyber-security/the-singapore-and-malaysia-government-connection-with-hacking-team-exposed-both-countries-using-spyware-for-digital-surveillance/) Why film innocent people doing nothing criminal in public places. Next, they’ll be putting them in public restrooms.
* “Those who give up liberty for safety deserve neither” – Benjamin Franklin. A camera everywhere is not a deterrent as all that’s needed is a mask. It will allow governments to watch us, which may not matter now, but in the wrong hands, can be catastrophic. We don’t deserve to be watched while living our lives.
* They don’t work. In New York a man got stabbed and was left to die in front of three surveillance cameras. It took the ambulances 2 hours to get to the injured man, and he died before getting to the hospital. The surveillance cameras did nothing to help the man.
* I think this is an awful idea because if a window is open somewhere, a person could look through and watch them all the time so that is an invasion of privacy.
* Police should be out on the streets trying to prevent crime. CCTV cameras are just a less effective alternative to having police walk the streets. CCTV cameras are just there to give the public a false feeling of safety and are a less effective replacement for policing.
* The myth is that CCTV cameras prevent crime but the reality is that they do not.
* [Internet connected IP cameras are of particular concern.](https://www.ifsecglobal.com/security/when-are-mp-ip-cameras-the-right-choice-for-hd-surveillance/) Such systems are more easily “hackable” than a closed circuit system and the concerns over cyber security only continues to grow.
* Where is the data stored that is captured, and for how long? Are all operators GDPR compliant?

## ****Governance and Governing Body****

In the ensuing debates over privacy versus safety and security, advocates on both sides would be wise to consider the following guidelines –

* **Responsibilities and Reasons:**We need to consider privacy issues when creating surveillance policies. For one, cameras should avoid or mask inappropriate views of private areas, such as yards and windows of bedrooms or washrooms.
* **Crime, Cost and Benefits**: Public surveillance camera systems can be a cost-effective way to deter, document, and reduce crimes. For example the cost savings associated with crimes averted through camera systems in a city of USA saved over four dollars for every dollar spent on the technology, while another city yielded a 50 cent return on the dollar.
* **Document and Publicise Policies**. The law enforcing agencies must formulate on how surveillance cameras can be used and what are the disciplinary consequences for misuse. Likewise, officers should be thoroughly trained on these policies and held accountable for abiding by them.
* **Forecasting and Post-Event Investigations:**The usefulness of surveillance technology in preventing and solving crimes depends on the resources put into it. The most effective systems are those which are monitored by trained staff, have enough cameras to detect crimes in progress, and integrate the technology into all manner of law enforcement activities. Use of correct video-analytics can actually raise alarms about crimes or accidents before they take place. Correct management software will help in tagging, archiving and retrieving the authentic data for post-event investigation.
* **Mix of Man and Machine:** People should be out on the streets and work-places trying to prevent crime or losses. CCTV cameras are just a less effective alternative to having police walk the streets or security personnel on patrolling and physical surveillance. As with any technology, the use of cameras is by no means a substitute for good old-fashioned ground work. The camera footage provides additional leads in an investigation and aids in securing witness cooperation. The video footage serves as a complement to – but not a replacement for – eyewitness evidence in the courtroom.

Using the estimate for the UK of five million CCTV cameras, that is over 43 billion hours of footage annually (5,000,000 \* 24 \* 365 = 43,800,000,000). Assuming one operator for every 10 cameras, each working an eight-hour shift, to review output live and act would require a staff in excess of 1.5 million. Clearly, there are not 1.5 million CCTV operators, many cameras are not monitored, but the footage recorded and used in later analysis. How long the footage is retained, who has access and how that is accessed presents some interesting Legal and Ethical challenges.

Retention periods are governed ….

Who has access is an interesting item, police and security services can request and access footage from other operators and in an investigative capacity (tracing a suspects movements whilst investigating a prior crime, or indeed acting on intelligence and aiming to prevent a crime) this would be almost universally acceptable. However, we must ask where is the boundary, with advances in Facial Recognition – does an expert operator need to be the one that follows the movements, or can a computer do this? If we accept that a computer can follow the suspect and report on their movements reliably – we now have an ethical problem:

Should we use automated image capture and facial recognition to inform and attempt to prevent crime?

Taking the scenario Person A meets Person B, Person B meets Person C and Person C then meets Person D (a suspected terrorist). Who are our persons of interest? What if Person A has been observed purchasing a certain chemical – should they be investigated?

Context is vital…. What if C was asking unknown D for directions – and Person A is buying for a legitimate reason? Correlation is not causation – need critical assessment as well as logical assessment of a sitation – therefore AI ??????

From a legal perspective, CCTV and related imagery is covered by the Data Protection Act / GDPR. Howeber, the covert surveillance activities of public authorities are not covered but rather they are governed by the Regulation of Investigatory Version 1.2 8 20170609 Powers Act (RIPA) 2000 and Regulation of Investigatory Powers (Scotland) Act (RIPSA) 2000. Critically this type of recording is covert and directed at an individual or individuals – so does not cover “mass surveillance”.