

Video security is a political animal

Technology does not exist in a vacuum and as much as it may exist as a tool for users, innovations will face scrutiny from outside parties. We have heard calls from groups such as Human Rights Watch and Big Brother Watch to ensure technology does not infringe upon people's rights or exacerbate pre-existing inequalities between groups. These viewpoints inevitably clash with companies needing to maintain the security of their properties, creating a complex balance between privacy and protection.

Temps de lecture : minute

22 November 2022

Life is political

The conflict between video security and privacy infringement often stems from how present it is in our daily lives. With over five million cameras in the UK alone, a person will likely be caught on video at least once every day. Something so prevalent in society ought to make people feel physically and mentally safe, without the fear of bias or mistrust. However, concerns still remain by some on whether these technologies are being fairly used.

Given the wide use of security cameras, it's impossible to do away with them in our current society. People and companies are striving to have greater protection and to know more. As such, eradicating this technology is not the most conducive to this. Even with privacy concerns, there is no doubt that video cameras safeguard the population by deterring criminals

and providing evidence should an incident occur. Therefore, it is the type of video security that is used and the way in which it is implemented that can alleviate the concerns some groups may have towards this technology.

The alternatives

A video camera is only as useful as the information it provides. For example, facial recognition can be inaccurate or unreliable and therefore open to criticism. We can remove (or at least mitigate) such concerns - while still maintaining data privacy - by finding alternative solutions.

Using security techniques such as motion sensors can detect human activity without scanning their face and mining their biometrics. At present, there are motion detectors that have the ability to anonymise people, thus protecting their identities and privacy while still maintaining the security of the location that they are installed in. Knowing where someone is, especially when they are not supposed to be there - such as on private property or at schools - is crucial for security personnel, who can then go and check what is happening on the premises they are charged with protecting.

Other analytical tools also exist that find a balance between privacy versus security. Utilising techniques such as a search box on the video management system, enables users to look for items - a hat or bicycle, for example - rather than people. The ability to search for objects means that individuals can still be identified, but not for their distinguishable attributes.

Going further, if a video camera is able to know if something is anomalous, it can alert security personnel or those monitoring the video management system. For example, if a person is in a shopping centre after closing hours, this unusual behaviour requires investigation. With

the help of technology, the security team would be able to find out whether it is just a customer who accidentally got locked in or something more dangerous. The video camera would be able to notify administrators of unusual activity before an issue happens, rather than them needing to find a cause retrospectively.

Now what?

While there are natural concerns towards the privacy of individuals when cameras are involved, there is no doubt that their use is important. Striking this balance goes beyond the number of cameras used in a single building and instead should aim to identify methods that improve the fairness of the security in place.

Sam Lancia is the cofounder and Head of Video Engineering at [Ava Security](#)

Article by Sam Lancia