PRIVACY VS SECURITY

Timothy Compston *wonders if the balance for CCTV and the sharing of suspect images has gone too far towards privacy to the detriment of time-critical policing and counter terrorism.*

The reluctance of certain European countries, like Germany and Sweden, to release pictures and footage of suspects – including those captured by video surveillance cameras – due to long-standing privacy laws and concerns, is, some would argue, impacting negatively on their ability to investigate and identify offenders after major incidents.

Regarding the way forward, the Christmas market attack in Berlin and how the pictures and name of the suspect were handled post-event have certainly generated numerous headlines and much subsequent discussion. This case serves to illustrate the different perspectives, operational procedures and legal frameworks at work here. Many commentators were critical of the fact that when the manhunt was underway for Anis Amri, pictures published in Germany had obscured elements of the Tunisian's face. By contrast, in Britain an unadulterated image featured prominently in the media. In addition, the German police continued to identify the person of interest as 'Anis A' rather than confirm his full name. Of course, it needs to be remembered that the German stance on the Berlin situation is being viewed through the prism of our experience in the UK where we have a long track record of pictures and CCTV footage being shared for public assistance and investigative purposes.

With credit cards and mobile phones leaving a trail of our movements, CCTV shouldn't be seen as an infringement of civil liberties

On the terrorism and public safety front, the value of having an extensive public space CCTV base – and less restrictive privacy requirements – is certainly well recognised on this side of the Channel. A recent case in point is the way that video surveillance helped the police and MI5 to track down and apprehend an individual near Westminster with "a rucksack full of knives". Over a decade ago CCTV images also proved their worth in a case related to the attempted attacks in London two weeks after 7/7. This evidence helped to support the convictions of four men for conspiracy to murder, a process assisted by nearly 28,000 hours of CCTV recordings gathered by the police. Fast forward to 2011 and CCTV was also at the forefront of investigations into the London riots with DCI Mick Neville from the Central Forensic Image Team estimating – two years later – that 4,000 of the almost 5,000 arrests were informed by CCTV evidence.

CCTV BEST PRACTICE

It is important to stress that, in comparison to the tougher regulations on mainland Europe, video surveillance in the UK is by no means a free for all, there are still specific requirements to be adhered to. Back in March, Tony Porter – the Surveillance Camera Commissioner – announced the launch of a national surveillance camera strategy for England and Wales to enable system operators to understand best practice and their legal obligations (such as those contained within the Protection of Freedoms Act, Data Protection Act and Private Security Industry Act).

Returning to the specific privacy situation in Germany, recent moves may signal that change is finally in the air. Last December, we witnessed the approval – days after the Christmas market attack – of a regulation to increase CCTV deployment in public places. Apparently, this step is designed to ensure that data protection commissioners lend greater weight to protecting life. It was stressed at the time that the new regulation was not a direct response to what happened in Berlin, but rather the culmination of an initiative the German interior minister had launched after the earlier Munich gun attack. Interestingly, the question of whether a CCTV scheme should be given the green light still lies at a local level with the relevant German cities and states.

Philip Ingram, a former British military intelligence officer, feels that how privacy works in relation to CCTV – and suspect images – is indicative of wider problems, especially in Germany and France, with the passage of intelligence and competing interests: "The privacy laws just make it more difficult. That is why, unfortunately, it is easy for people to slip through the net. In Germany, the intelligence agencies at a local level who work with the local police won't necessarily talk to those who are responsible for the state and the state police, and they won't talk to the Bundespolizei and the Bundeskriminalamt". Ingram also points out that another gap in Germany is the lack of a central criminal database where information is shared: "Often they [the police/intelligence agencies] keep information close to themselves and won't pass it across," he concludes.

On the question of whether there are technological advances coming down the track that could potentially help to bridge the gap between privacy protection on the one hand and counter terror and crime fighting on the other, Stephan Sutor – who co-founded Kiwi Security – is keen to flag up the difficulties involved. He points to the reality that in Europe privacy requirements are still very different, not only from country to country, but often within a country: "This is valid for Germany or Switzerland where there are state-level laws, which make it very complex to have general guidelines or rules because there are really small differences in detail. If you go to Germany and you want to do something in Hamburg, the privacy or the data protection officer might tell you: 'I don't care what the guy in Munich said because this is my state and we do it this way'". Sutor adds that there are different initiatives coming down the track, including the new privacy directive from the EU to try and harmonise and standardise these efforts.

Drilling down to where technology can have a role in transforming how privacy and security concerns are addressed in the context of video surveillance – an area where Sutor's expertise lies – he believes that these often competing interests can be reconciled through video analytics. Sutor points to the contradiction at work here: "You want more privacy, but you have to sacrifice security or you want more security and you have to sacrifice privacy". For Sutor, and his colleagues, the aim has been to come up with more "creative and intelligent solutions" to "bust this old contradiction", against the backdrop of privacy laws and directives passed in the European Union and similar policies in other parts of the world: "We need to deal with the fact that once we are putting cameras up and filming people, we are entering their personal privacy," he notes.

CCTV INTRUSION IS NOTHING COMPARED WITH WHAT IS WILLINGLY SHARED ON SOCIAL MEDIA

BLURRING THE FACTS

Asked whether it is enough to simply blur an individual's face, from experience developing Kiwi Security's Privacy Protector solution, Sutor notes: "Personal data isn't just your face. You can be identified by the way you walk, for example, or tattoos and jewellery, so we pixelate or blur the entire person". He explains that this process happens, automatically, in real-time so it is still possible to recognise actions, what people are doing, without giving up their identity. "It is only after the fact if something bad happens that 'super users' can access the original video and export it for evidential purposes." In the end, the message from Sutor is that it is now possible to use technology in an intelligent way to enhance privacy rather than simply to lessen it.

Heading East, for a Scandinavian perspective on privacy and video surveillance, Martin Gren co-founder of Axis – a pioneer in network video

products – reveals that in his native Sweden today few, if any, public space video surveillance cameras are in evidence: "In all there are only 120 surveillance cameras operated by the police, which is probably less than you might have in a single borough of London".

Outside of Sweden, when events unfolded in Cologne, Germany, a year-and-a-half ago, Gren notes that there was a similar picture with hardly any cameras to assist public safety. So why is there such a dearth of cameras to monitor outside areas in towns and cities? Gren says that some of the privacy issues around video surveillance preventing wider deployment in Sweden, Germany and elsewhere are a throwback to 1984 when the CCTV camera came

IT IS NOW POSSIBLE TO USE TECHNOLOGY TO ENHANCE PRIVACY RATHER THAN SIMPLY TO LESSEN IT

to symbolise the notion that 'Big Brother is watching you'. Times have, however, changed says Gren, and he believes that this sort of thinking is outdated and we should no longer be talking about Big Brother in terms of people watching each individual surveillance camera 24/7. "They [cameras] were super expensive in the eighties so every camera you put up had an operator. Today as we all know 99 percent of video is never watched and if someone leaks a surveillance video it is, typically, a reason to fire them," he says.

Taking a wider view, Gren argues that the implications for privacy that come with video surveillance cameras are nothing compared to what is being shared willingly all the time on social media and elsewhere: "This is 2017. We have social media, we have Google, we have credit cards, and we have cellphones. Cellphones are tracked so they know where we are. With social media, we give out all our privacy – who our friends are, what we tell our friends, what our friends are doing, and what we are doing – and the credit card system in Scandinavia is almost cashless so all our financial transactions are also logged".

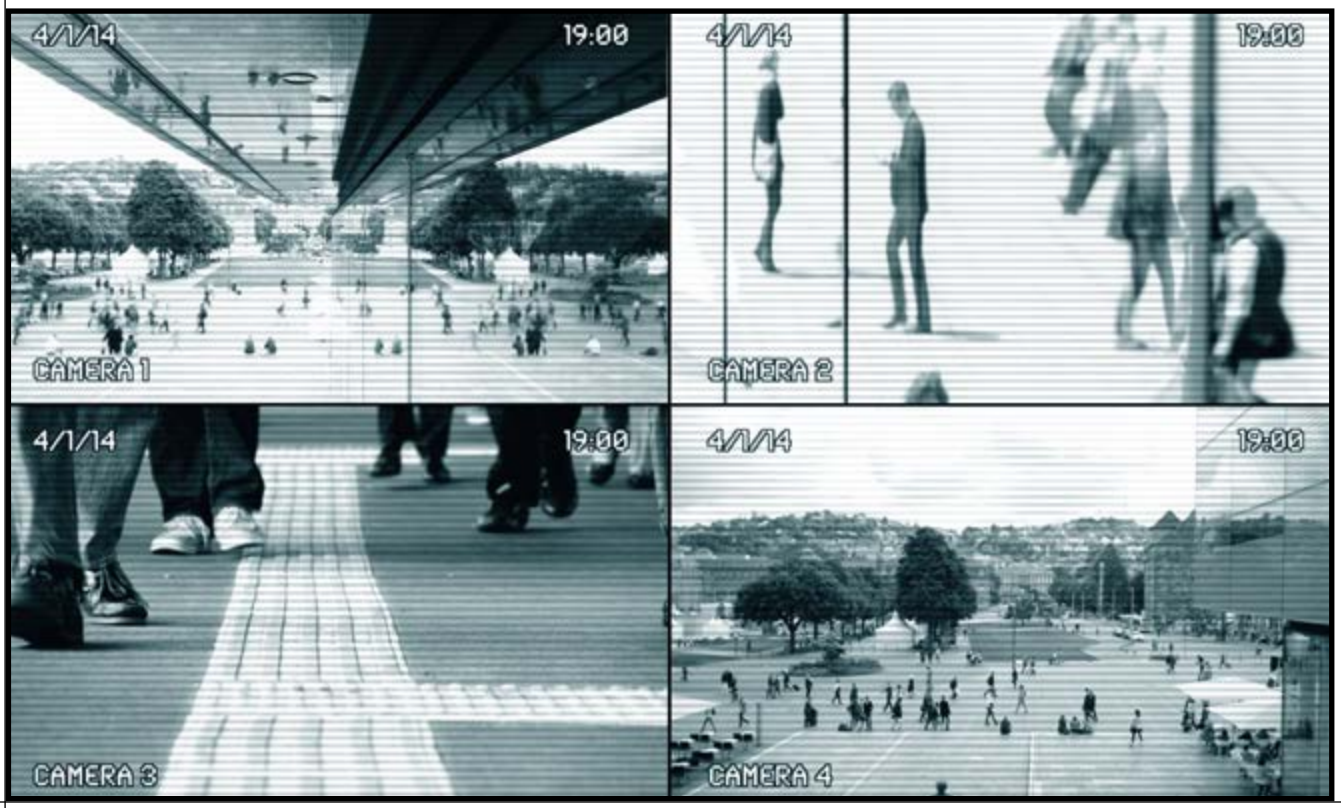
CHANGING MINDS

Gren continues that while the public is aware of the changing dynamic on privacy, unfortunately, politicians are behind the curve and still want to regulate what they can regulate: "In Sweden we are one of the few countries to have a camera-specific law [Swedish Camera Monitoring Act (2013:460)]. The law was intended to protect our privacy and integrity when it was created. However, today the real integrity issue can hardly be that of the security cameras, as we give out so much to social media, Google, cellphone operators and credit card companies who know everything about us!"

As a proponent of CCTV, Gren points to the findings of a SIFO survey conducted in 2014, which found that 92 percent of the Swedish population are positive towards surveillance cameras in certain public places. Various events in Sweden over the last few years have invariably brought discussion on the utility of CCTV cameras for public space surveillance to the fore again. Interestingly, as a sign of new thinking, Gren tells me that the police are now more willing to release video from surveillance cameras to get assistance with catching offenders.

Moving ahead, it will be interesting to see the trajectory that privacy, crime fighting and counter terrorism takes both in mainland Europe and the UK. Will the authorities across Europe decide to relax their more stringent privacy requirements considering the heightened threat level? Are we likely to witness, for example, an expansion in the footprint of video surveillance solutions to monitor public spaces? ●

Timothy Compston is a journalist and PR professional who specialises in security issues. He studied International Relations at Lancaster University, is PR director at Compston PR and a previous chairman of both the National PR Committee and CCTV PR Committee of the British Security Industry Association.



CCTV still has a vital role to play in public safety and security

Picture credit: Getty