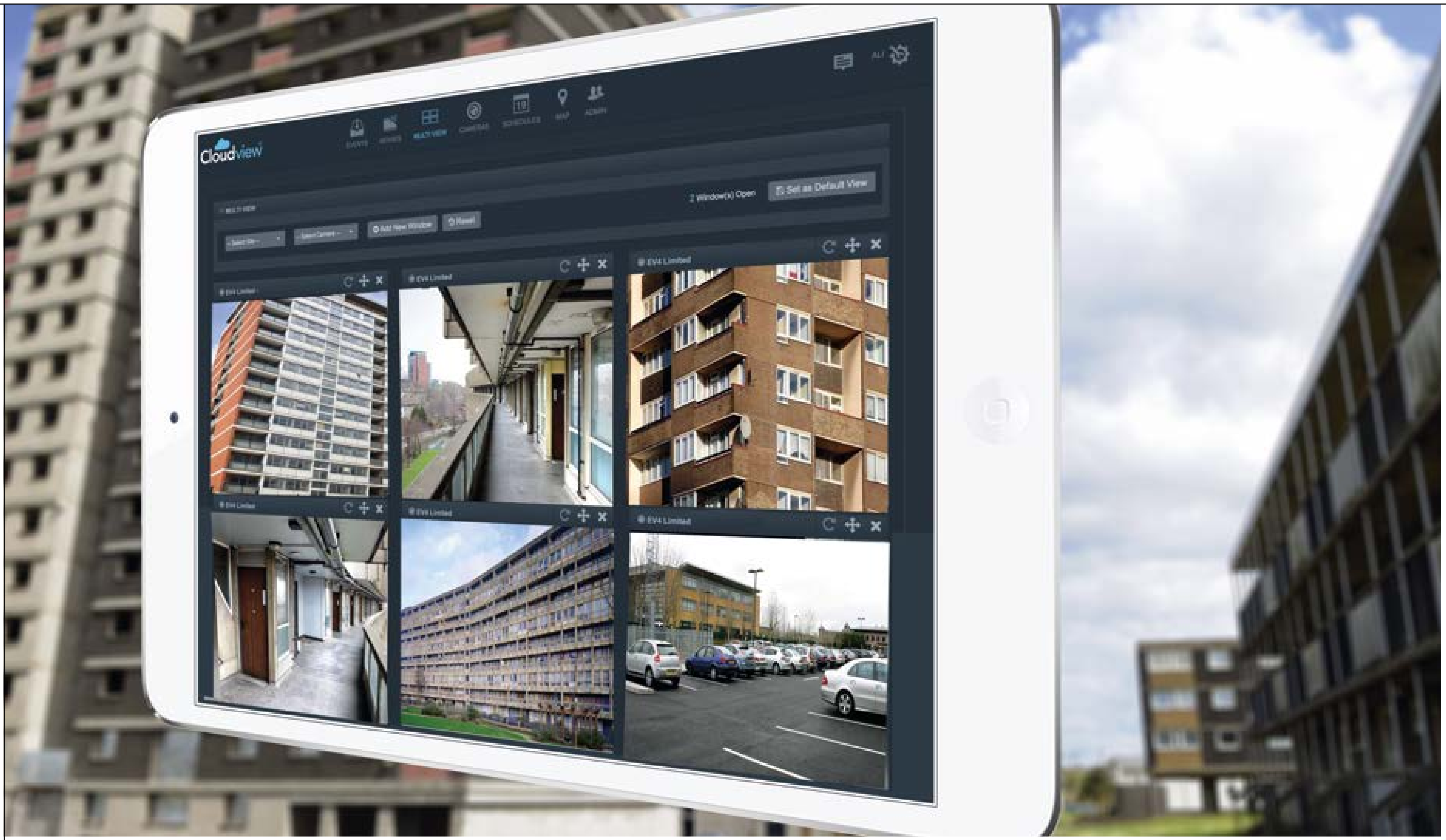

Specialist systems offer overview and control of CCTV cameras

Picture credit: Getty

IS BIG BROTHER REALLY WATCHING?

James Wickes *investigates if CCTV and surveillance are a protection measure or an invasion of our privacy*

CCTV has become one of the *de-facto* technologies used for the protection of people, property and assets. It's everywhere – in shopping centres, offices and public transport, you name it. Yet questions are still raised about its effectiveness and considerable public unease remains over the implications of its use on privacy. Research figures from the British Security Industry Association (BSIA) show that the UK has more than 6 million CCTV cameras deployed, equating to one camera for every 11 people. When you start to count the cameras perched on car dashboards and cycle helmets as surveillance cameras, the numbers go off the scale.

Furthermore, the UK's Metropolitan Police has recently introduced body worn cameras in what is believed to be the largest roll out of its kind anywhere in the world. The Body Worn Video (BWV) cameras are being issued to over 22,000 Met frontline officers, including overt firearms officers, across all of London's 32 boroughs.

By nature, CCTV systems can only be effective if they record information accurately, and that information can be found and legitimately used before it is out of date or recorded over. So the big question is: are the many organisations that use CCTV actually able to access the visual data their systems record quickly and effectively when needed? And can they get it to the authorities in a timely fashion and in a format that is usable as evidence? There are nagging doubts about the monitoring, quality and use of CCTV images and videos, to such an extent that the Metropolitan Police has been recently criticised for failing to solve crimes because they are not investigating CCTV footage in a timely manner – sometimes not at all. Mick Neville, a former detective chief inspector and head of the Central Forensic Image Team at the Met, recently claimed that despite billions of pounds being spent on CCTV cameras by companies and individuals, images were not routinely collected by police. In fact, images were collected for a mere 1.9 percent of crimes.

This tells us that the key issue is not a lack of surveillance cameras or CCTV footage recorded by them. Rather, it is the ability to get that CCTV footage to the police quickly (or at all) that has become the problem. Most CCTV footage is recorded onto 'local' NVRs or DVRs and is not easily accessible. Incredibly, an authorised person that knows how to use the CCTV equipment has to physically go to where the DVR or NVR is located, find the relevant footage and then put it onto a disk or USB stick so the police can collect it for review. This can take many hours (assuming the equipment is working in the first place). If the user is unable to download the footage from their system, the police frequently end up taking the entire recording set up as evidence. All except the most lavish CCTV systems do not provide functional oversight so the hapless user can often find their CCTV equipment is out of order, and there is no recording.

> THE UK HAS MORE THAN 6 MILLION CCTV CAMERAS, WHICH EQUATES TO ONE FOR EVERY 11 PEOPLE

So it's no wonder the police are not using CCTV footage in the pursuit of crimes. They simply don't have the time to waste on retrieving it.

FINDING A BETTER WAY

Is there a better way? Yes – by using a technology that has already revolutionised many other areas of IT – the cloud. This enables organisations to transfer and store all their CCTV data in the cloud where it can be processed, managed and accessed on demand by authorised users – just like the data from their other IT systems. There are also more advanced features on offer from cloud CCTV service providers that can take visual surveillance beyond the bounds of conventional CCTV, improving both its effectiveness and accountability.

Strategic automation – organisations can connect their legacy CCTV to the Internet of Things (IoT), so there's no need to "rip and replace" cameras or cabling. Equipment performance can be monitored and users can be automatically informed of equipment failures. Additionally, such systems can be integrated with external alarm sensors and device actuators. Interactivity with other IoT devices provides the opportunity to create smart environments where security is part of a bigger picture.

Advanced security – the latest cloud systems encrypt CCTV data from end to end and include measures to prevent unauthorised access or hacking. Data from existing analogue or digital CCTV cameras is transmitted securely to the cloud via an encrypted tunnel. Once stored, the data is fully encrypted. Furthermore, the loss of visual data can be prevented as many cloud systems completely negate the need for onsite recording equipment which are prone to theft, damage and mechanical failure.

Functionality – measures can be taken to record only what is required. The recording parameters of individual cameras can be easily adjusted, or cameras may be switched on or off at any time, to ensure compatibility with purpose. Some cloud systems also provide the additional benefit of motion-based recording so visual data is only captured when something relevant is happening. Video and sound can be recorded as separate files to avoid mistaken use. Visual data can be located and then viewed using pre-defined search criteria and parameters to reduce the amount of footage that requires reviewing.

Flexibility – access to visual data by authorised users is instant, allowing issues to be reviewed and effectively responded to. Real time and historic footage can be viewed remotely by authorised users from any location using smartphones, tablets or PCs. Links to original footage can be emailed or footage can be downloaded to provide evidence to the police or other authorities when necessary.

What's also clear about CCTV systems is that there are major risks to privacy. We know the potential benefits of CCTV, but how are organisations implementing CCTV managing the data they record?

Privacy – which is often compromised by poor cyber security – is a topic frequently featured in the national news. The highest profile casualties to date were the customers of TalkTalk, who was fined a record £400,000 by the Information Commissioner's Office (ICO) for its poor data security following the theft of personal data belonging to 157,000 customers in October 2015. On a surveillance level, the consequences of being ignorant are bleak too. The ICO recently warned that businesses could face fines for ignoring CCTV data protection law after a business owner using in-store CCTV was prosecuted for failing to register with the ICO.

Incidents where personal data has been stolen, lost or subject to unauthorised access are now commonplace. Worryingly, many of these incidents are caused by data being inadequately protected by the organisation storing that data.

This loss or theft of data poses a serious threat to the privacy of data subjects (you and me), and continued reports of data breaches are eroding public confidence in the ability of companies and public services to secure personal data and ensure that it is being used for its original purposes. Just as with any other data, organisations that inadequately protect the visual data they collect are in breach of the current Data Protection Act (DPA).

The penalties for the abuse of personal data will increase substantially when the new General Data

Protection Regulation (GDPR) comes into force on 25 May 2018. Serious breaches of this legislation could lead to fines of up to €20 million or 4 percent of global turnover, whichever is higher. These increased fines will apply immediately, so organisations need to take steps right away to ensure that their surveillance systems are secure and compliant along with their other data systems.

GETTING IT RIGHT

Management will be required to set out procedural frameworks in the use of CCTV for their employees to demonstrate compliance. Yet, due to the inherent limitations of traditional CCTV, these frameworks will likely impose blanket restrictions on access to CCTV data rather than allowing access to specific data by specified employees (as is the case with most IT systems). Moreover, companies wanting to avoid the disruption of an investigation and big fines by the GDPR authorities will also want to have comprehensive oversight of the operation of their CCTV systems and the data held on them. This may be possible with one or two CCTV installations, but not without increased manual intervention on the one hand and lock down on the other. This makes CCTV more resource hungry and less productive.

The incapacity of traditional CCTV can be easily remedied by connecting them to cloud-based CCTV systems. Cloudview for example connects incumbent CCTV cameras to its service with a simple low cost adapter. Once up an running, it's possible to get a complete overview and control of all CCTV cameras connected to the service. This means that organisations will subsequently find it far easier to comply with the GDPR while getting a more accessible, more secure and flexible CCTV system.

One organisation already using a cloud system successfully is Family Mosaic. This housing association, which manages 26,000 rented properties and provides 8,000 people with housing, care and support services, uses CCTV at many of its sites to help protect property and residents from anti-social behaviour such as vandalism and fly tipping. When there was a recent issue with someone accessing one of its properties to try and steal mail, the Neighbourhood Manager was able to send CCTV footage to the police remotely and immediately so the culprit could be identified. In the past, it could take the police up to two weeks to collect a USB stick for the same purpose.

Being able to access the system from any location also means that individuals, that may be carrying out the anti-social behaviour, do not realise that CCTV footage of their activities is being reviewed. In some cases, it can be dangerous to go on site to access the DVR as the offenders may want to prevent the organisation obtaining the evidence. Now Family Mosaic can look at the video in real-time from any location or provide access to the police if appropriate.

> THE ABILITY TO GET CCTV FOOTAGE TO THE POLICE QUICKLY (OR AT ALL) HAS BECOME THE PROBLEM

To summarise, CCTV needn't be the nosey big brother. When used in the right way, it can effectively protect people, property and assets – and give much-needed reassurance to the public that it is there to protect us, not invade our privacy. It is time for CCTV systems to catch up with the rest of the IT world with secure cloud technology. It is the pain-free way of enabling organisations (and the police) to improve the effectiveness, security, accessibility, privacy and most importantly the accountability of their CCTV systems. There really aren't any catches so there's no need to get caught out ●

James Wickes – CEO and co-founder, Cloudview. He is a serial entrepreneur with 30 years' experience in IT. In 2012 he launched the world's first corporate-grade, secure, cloud-based video surveillance system – Cloudview – where he is CEO and co-founder.

Using the cloud provides a superior way to access footage from CCTV cameras