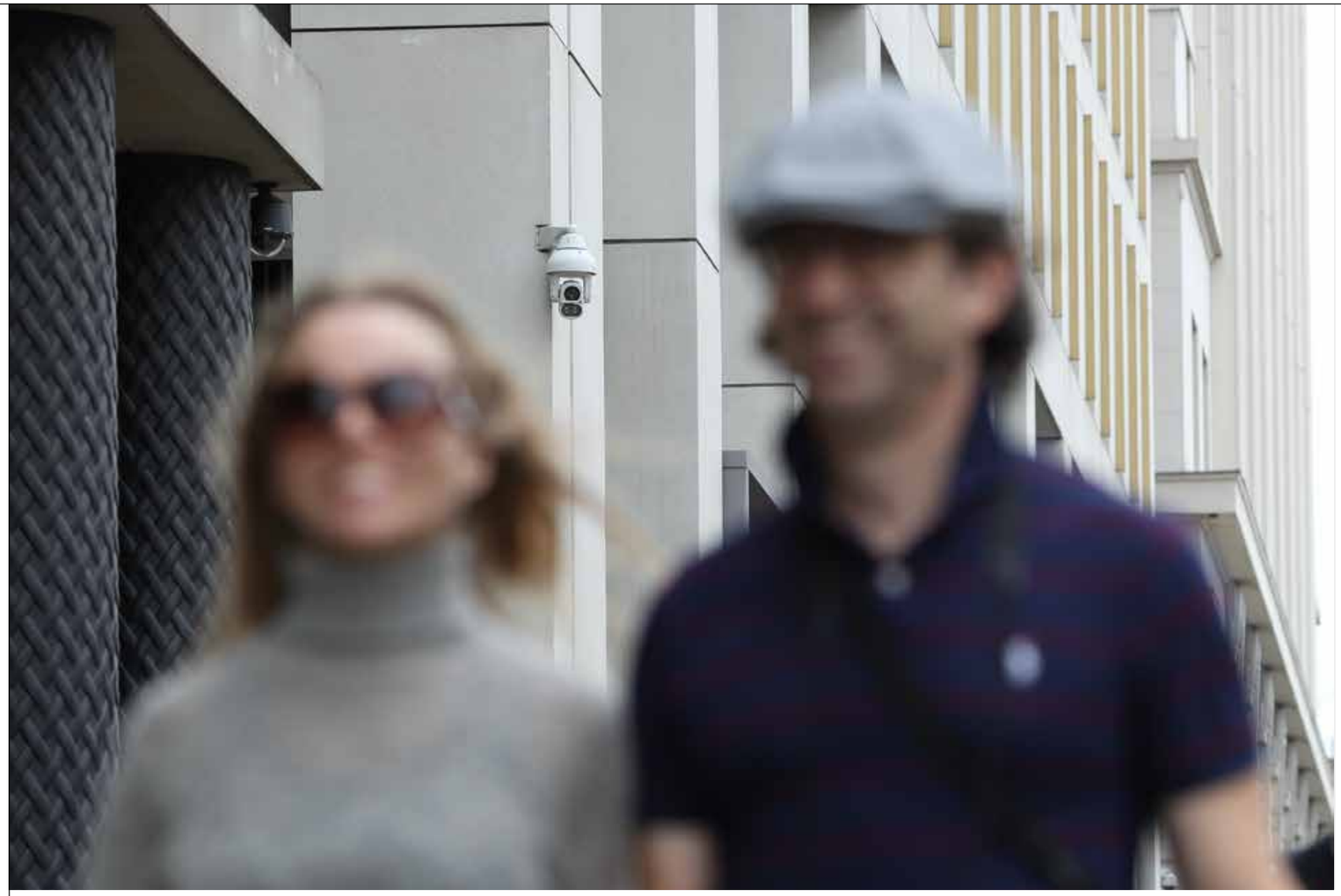


Picture credit: Getty

ANONYMISED SECURITY

Neil Huntingdon *explores the growing disharmony between data protection and mass surveillance and the role technology can play in balancing public demand for privacy and security.*

If you've picked up a paper or watched the news even once in recent weeks, it's likely you'll have come across at least one of a stream of headlines relating to public concerns around privacy. This July, the UK Home Secretary (and now chancellor) announced his support for police trials of facial recognition cameras, in spite of current legal action being taken by a shopper who was inadvertently screened by a police van in a Cardiff street. His case, which has received backing from civil liberties group Liberty, argues that the use of the technology without prior consent is a fundamental invasion of privacy.

Because automatic facial recognition (AFR) produces a biometric map that's uniquely identifiable to the individual, it is more like DNA and fingerprints than CCTV as a method. However, there is no specific regulation governing how police use facial recognition or manage the data gathered.

There is no regulation governing how police use facial recognition or manage any data that is gathered

Liberty has argued that even if it was regulated, facial recognition breaches human rights and should not be used. AFR has also received criticism from other UK sources, including South Wales Police, which has placed it under judicial review, and the information commissioner, Elizabeth Denham, who has criticised "a lack of transparency about its use". Tony Porter, the surveillance camera commissioner, also intervened in its use recently by stopping Greater Manchester police from using it at the Trafford shopping centre.

Whatever your view, privacy is high in the news agenda, and this is arguably a result of a heightened global terror threat, the rise of cyber crime and the introduction of GDPR and other directives across Europe and beyond.

THE GDPR FACTOR

GDPR in particular has triggered a dramatic attitude shift and increased public awareness around privacy issues and the use of personal data. This has cast a spotlight on more traditional surveillance methods, particularly CCTV. Indeed, storing recorded security footage has long been considered the same as storing personal data under the Data Protection Act, but the advent of GDPR has underlined this further.

This imposes more stringent requirements and responsibilities on CCTV users, whether they represent the police, armed forces and local authorities or private businesses, retailers and individuals. For example, users must be able to justify their requirements for CCTV and the areas being covered, and data subjects picked up by CCTV have a right to know they are being recorded and why. The data collected must also be stored appropriately, and only for as long as is appropriate.

It has also led to increased costs for CCTV users – redacting or 'blurring' facial features and vehicle license plates in video clips can be costly, with recent commentary suggesting it takes up to eight hours to process a single minute of surveillance footage.

This climate of scrutiny could present challenges for the industry. But, with challenges come opportunities.

According to Mintel's latest *Security Equipment Access Control And CCTV* report, the UK's security equipment market has shown consistent growth over the past decade, and it's now valued at around £4-billion. Such resilience sets this industry apart from most others, which have all felt the pinch of uncertainty following the EU referendum.

The report points to two reasons why it has continued to boom in the UK especially. Firstly, police numbers have fallen significantly, with Mintel quoting a decline of almost 15 percent between 2009 and 2018. This coincided with an overall reduction in Government expenditure on public order and safety.

Secondly, the decline accompanied an increase in criminal incidents: vehicle thefts in the domestic sector rose by 8.4 percent in the year up to 2017/18, while damage and arson increased year-on-year for the five years up to 2018. The commercial sector has also been a victim of this trend. During 2017, burglaries reported by businesses more than doubled, while the average cost of shoplifting to each victim increased from £237 to £500 between 2012 and 2017. These trends have had severe consequences on public life, including a noted decrease in visible deterrents, such as police constables, and reduced confidence in the state, according to polls.

However, there is another reason for growth across the surveillance industry: innovation. Thanks to increased access to digital connectivity, surveillance and security technology is evolving rapidly, and this is placing new demands on the sector for enhanced products and capabilities. This evolution is taking many different forms and using all sorts of platforms, from drones to social media. Recent examples include supermarkets using facial recognition to verify the age of customers buying alcohol and cigarettes and a video surveillance service for taxi passengers. The intention in all of is to prevent crime, deliver justice and keep people safe. But, could such applications fuel further fear and distrust?

LIDAR CAN BE USED TO DETECT PATTERNS AND IDENTIFY TRENDS IN CROWDED ENVIRONMENTS

There are other challenges too. As technology gets increasingly smarter, more digitally integrated with other devices and more widespread in use, how are users' networks going to cope? Where is all the data going to be stored? And how are the regulatory requirements of hosting all this data going to be managed? The answer lies in balancing this set of requirements in a way that maximises privacy, prioritises critical information gathering and minimises data production and storage need.

One solution already exists. Most commonly associated with the automotive sector and the development of driverless cars, lidar uses an array of lasers to detect objects, people and vehicles. Unsurprisingly, it has many applications, including surveillance and security.

With the unerring accuracy of lasers, lidar combines the imaging capability of the camera with the ability to function in various weather conditions, day and night. Lidar solutions can also be developed to produce 3D as well as 2D scans, providing a complete image of the world around it using data points rather than actual footage.

Most importantly, lidar sensors can work in partnership with advanced perception and business logic software to solve complex problems and perform specific tasks. This can be especially useful in the surveillance and security space where it can be teamed with software to detect, track and classify objects such as people or vehicles within user-defined virtual exclusion or inclusion zones.

This capability has been enhanced by building an advanced perception software platform that allows data to be processed immediately at the sensor site. This runs on an edge computing device integrated with the lidar hardware allowing the technology to be used to highlight only potential threats, such as an intruder or a suspicious package. This then limits the surveillance of those not involved in any suspicious incident.

Lidar-based detection, tracking and classification systems allow for far greater protection of data, because they enable operators to zero in on possible issues in a way other technology cannot. They build comprehensive images of the objects within their range, but not to the extent that biometric data or physical qualities can be collected.

Because the approach is to perform point cloud real-time processing "at-the-edge", lidar surveillance systems can reduce the network bandwidth overhead. A typical system outputs a stream of metadata, which is represented in kilobytes – something that differs greatly compared with the raw point cloud output of tens of megabytes per second. This prevents networks from being overloaded and reduces the cost and management requirements behind data storage, making the solution easily scalable as well as suitable for mobile applications. What's more, if it's set up to trigger CCTV surveillance at the point of an incident, it can help reduce the volumes of sensitive video data being collected and stored by users.

Lidar also fills the gap when it comes to medium-range detection. As a complementary technology, it's environment agnostic – ie it operates reliably in adverse weather and lighting conditions, and isn't subject to electromagnetic interference. It also 'sees' and builds visuals in 3D, which can then be overlaid onto video footage to provide an even more accurate assessment of the threat and any related access or exit points. In fact, work is currently being carried out with network camera manufacturers to integrate lidar into their products in order to further enhance their accuracy and intelligence.

SUBJECTS PICKED UP BY CCTV HAVE A RIGHT TO KNOW THEY ARE BEING RECORDED AND WHY

Finally, lidar is smart and highly accurate when it comes to minimising false positives and false negatives. With an in-built computer, it can analyse and respond to data triggers at speed and can even be used to detect patterns and identify trends in crowded environments.

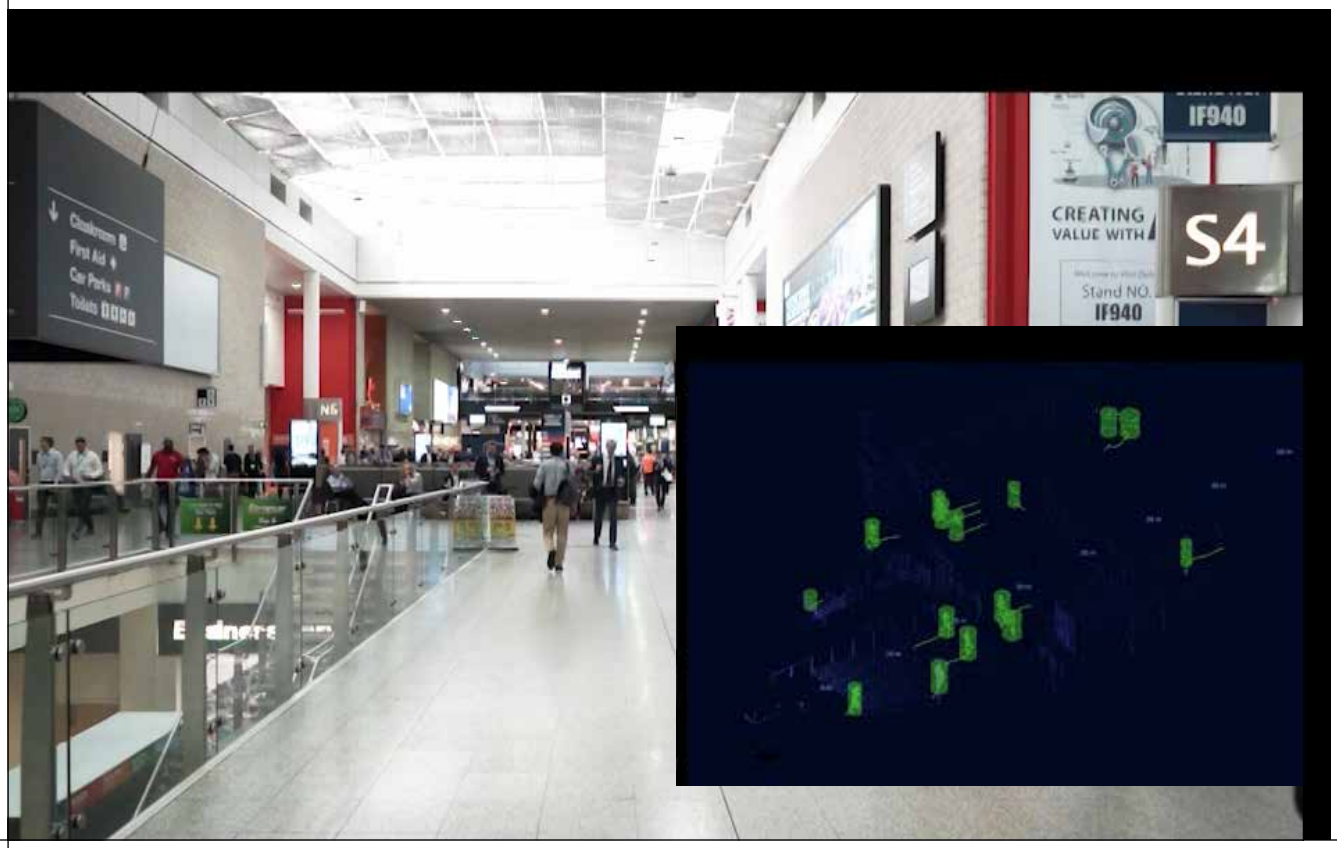
MULTI-PURPOSE DETECTION

Clearly, lidar-based detection systems have many use cases. In airports, train stations and ports, for example, it can identify trespassers in forbidden or no-return areas and detect unattended or abandoned luggage or packages. At large sports and music venues and theme parks it can track trends in movement, crowd behaviour and congestion, allowing for remedial action and improvements in customer experience. Similarly, in industrial or critical environments it can detect unauthorised activity such as break ins or accidents by monitoring movement and activity in exclusion zones.

These are just a few examples that demonstrate how lidar works as a novel surveillance technology to address mounting concerns and growing mistrust in surveillance and data protection. While it will never replace the need to be able to identify guilty parties and other threats in order to deter crime, prevent harm and deliver justice, lidar is a complementary system that enhances traditional approaches.

Not only does it address many of the issues around data storage and management, it also allows us to protect the anonymity of people or objects that are not deemed to be a threat. This is a step-change from existing technology, where everyone's face is captured and held on video storage, regardless of whether they were involved in an incident or not ●

Neil Huntingdon is vice president of business development at Cepton Technologies Inc – a leading provider of lidar technology to the automotive, security, transport, critical infrastructure, industrial and mapping industries.



Lidar can track trends in movement, crowd behaviour and congestion

Picture credit: Cepton Technologies Inc