TIME FOR CHANGE

James Wickes *reveals how the GDPR can help to transform our use of visual data*

Any mention of CCTV surveillance is likely to call up images of grainy video footage being used to spot law breaking or suspect behaviour in public spaces and business premises. And indeed, some of the UK's cameras do exist purely to protect public safety.

There are more than 6 million cameras in the UK not including all the dashcams and home security cameras that are growing in number all the time, and between them these do a great deal more than just surveillance duty. Cloud technology is enabling a whole new range of roles helping industry, healthcare and other sectors to use visual data in ways that can improve efficiency and enhance safety.

For the sector to grow and develop as it should, adequate regulation is required. At the moment, regulation in the UK is provided through the Data Protection Act 1998. *Watching the Watchers*, a White Paper by Andrew Charlesworth, reader in IT and Law and Director of the Centre for IT and Law at the University of Bristol (CILT) points out that this legislation has been criticised for its lack of focus on accountability.

IT'S UP TO THE INDUSTRY TO SEE THE GDPR NOT AS A SERIES OF OBSTACLES, BUT AS AN OPPORTUNITY

However, the importance of accountability in data protection legislation is about to change dramatically. In May 2018 the Data Protection Act 1998 will be replaced by the General Data Protection Regulation (GDPR). This will become law in all EU member states without the need for legislation. Brexit is not likely to have any effect on this.

The arrival of the GDPR will place new requirements on those that collect and manage the visual data that cameras generate. Data controllers and processors will need to be more accountable for the data they store and use. Meeting the requirements of the GDPR will require some significant changes to the approach organisations take to managing CCTV and other camera systems.

This compulsion to change gives the sector a rare opportunity to take a long, hard look at itself and undertake the kind of work that, if handled properly, could be transformational on multiple levels.

There are some key areas in which the GDPR can empower the visual data sector to take the initiative and use its requirements as a spur to greater things. Taking responsibility for good practice around the data that is generated – and being seen to take that responsibility – is one of these. Addressing the data security issues that can be so damaging to the sector both in its effectiveness and to its public image is another. And a third is embracing new technologies, most notably the cloud, to drive the development and delivery of new services and meet the GDPR's compliance policies.

TIME FOR ACCOUNTABILITY

The GDPR represents a significant shift in UK data protection legislation taking it away from a compliance culture and towards one based more around accountability. Specific provisions within the GDPR require a greater degree of active management around accountability than is found in the Data Protection Act 1998. For example, there is a requirement for Privacy Impact Assessments (PIAs) to be produced for what the GDPR refers to as "high risk" processing. It mentions specifically large scale, systematic monitoring of public areas.

PIAs will require a number of components including a description of the purpose of data processing and an assessment of its necessity, an assessment of the risks to the rights and freedoms of data subjects and details of measures that will address those risks such as safeguards and security mechanisms. Moreover, a PIA can't be simply produced by the data controller or data processor in its own silo and handed to data subjects as a point of information. It needs to include the views of data subjects or their representatives.

The requirement to produce a PIA might be seen by some as an administrative burden. But instead it should be seen as an opportunity. A well-constructed PIA can be a way to build relationships with data subjects and the wider public.

A similar case can be made in relation to other requirements of the GDPR around accountability.

Picture credit: Getty

There are now more than 6 million cameras in use in the UK alone

They give the industry opportunities to show initiative, display greater public transparency and evidence their commitment to regular review and evaluation of policies. It may even be appropriate to enhance accountability-based activities beyond the requirements of the GDPR.

Such actions could go a long way towards helping repair damage done by negative perceptions of CCTV as part of the surveillance culture and help dispel preconceptions that visual data is collected for secretive, controlling or other negative big brother-style purposes.

The technology used in CCTV systems has come on in leaps and bounds in recent years. Where once the only options were built on closed circuit, wired systems that recorded data onto digital video recorders (DVRs), we are now in a world where both IP and analogue cameras can send footage directly to cloud storage, which can be accessed from any location, at any time.

While the options cloud storage offers are far greater than those found on DVRs, both systems and cameras themselves can have vulnerabilities, which may result in serious consequences under the GDPR.

Some CCTV systems are very poorly secured. It is relatively straightforward to find IP addresses for devices using dynamic DNS and many DVRs use fairly easily identifiable domains. Just last year, a Cloudview-sponsored research project tested

50,000 domains for one DVR maker and within a few minutes identified 2,400 valid domain names, around 14 percent of which were running some kind of open service. Once a device is found, applying default user names and passwords can be surprisingly effective at gaining access.

DENYING ACCESS

Moreover, firmware updates are far from ubiquitous for DVRs and cameras as older firmware can leave devices even more open to further vulnerabilities. One doesn't have to look far on the web to find sites streaming data from poorly secured cameras. More insidious people can compromise CCTV systems to contribute to botnets or use them as access routes to corporate networks.

The GDPR is clear that a CCTV user or provider installing a new system or upgrading an old one will need to identify security risks and measures to address them. The industry could make a significant move by taking this responsibility further and going beyond the requirements of the legislation. One approach that could have substantial effects is supporting measures to create kitemarks for cameras and data storage systems to meet a set of standards. This would put the sector on the front foot where data security is concerned and should eliminate services with poor security.

BREXIT IS NOT LIKELY TO HAVE ANY EFFECT ON THE GENERAL DATA PROTECTION REGULATION

As storage of visual data moves more to the cloud, so the potential for a whole new raft of camera-based, data-driven services opens up. We are already familiar with security cameras that can send alerts to mobile phones and enforcement agents when unexpected movement is detected. But this is just the tip of the iceberg of possibilities.

When visual data from individual cameras is combined and appropriate analytics are applied, a whole new world of ways to improve the way we live and work opens up. Cameras could, for example, be used to help streamline workflow and the movement of people and objects on the factory floor. In hospital A&E departments or operating theatres, they could record how people move around to determine the ideal location for particular equipment in situations where quick access is vital.

Visual data from roadside and in-vehicle cameras could be combined (shared with appropriate consents, of course), to produce detailed records of traffic accidents and to alert emergency services when incidents occur. Workplace cameras in hazardous environments could spot dangerous situations, with the appropriate authorities automatically alerted. Thanks to facial recognition, cameras may even make ticketless travel possible.

The list of opportunities is mind-bogglingly extensive, and technologically within our grasp. Such a broadening of the role of visual data takes it beyond pure surveillance and into a world where it is an enabling technology.

IMPORTANCE OF THE CLOUD

The cloud is both central to these exciting new uses for visual data and the technology that makes the implementation of GDPR compliance policies workable. As visual data becomes 'big data', features of cloud technologies allow data controllers and data processors to ensure compliance. In fact, the cloud is the pivot around which compliance and new service development turns.

The number of CCTV cameras in the UK will surely continue to grow. The use of IP cameras linked to cloud storage for domestic security purposes is in its infancy, and this area looks set for exponential development. Meanwhile, the traditional public security role continues alongside a growth in the use of visual data that may be focused on both people and objects.

It's up to the industry to see the GDPR not as a series of obstacles, but as an opportunity to rethink the way visual data is stored, address concerns about how it is secured and ultimately work through the possibilities of how it can be used to better effect as a business tool rather than purely as a security system ●

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

Swift action could give CCTV a more positive public perception