ic2 DESIGN INSTALL PROTECT

CCTV, the ICO and the DPA: Tightening compliance through increased regulatory power

A discussion of likely changes to the regulatory framework governing the storage and use of personally identifiable information

www.ic2cctv.com

Regulation behind the curve of technological change

Over the last decade or so digital technology has steadily enhanced the capability of CCTV. The use of the latest systems means we have never been more able to identify individuals through CCTV than we are today. Technology moves faster than the legislation, and it is only to be expected that the regulation of CCTV and the personally identifiable information it generates has been somewhat behind the curve.

The first guidance, which predates the widespread use of digital CCTV technologies, was issued in 2000 under the Data Protection Act (DPA) 1998. This remained definitive until October 2014 when a long overdue overhaul of best practice and the regulatory code for security and surveillance systems was issued.

'In the picture: A data protection code of practice for surveillance cameras and personal information' was published clarifying the role of the Information Commissioner's Office (ICO) in regulating the use of CCTV and identifying places where it touches the DPA.

However, while no one expected it to be another 14 years before it would need overhauling again, few could have thought circumstances would arise requiring it to be re-visited within a year or so. But that is exactly what happened.

TalkTalk, the ICO and that data security breach...

The TalkTalk data security breach that occurred in October 2015 exposed the personal details of 155,000 customers and enabled criminals to successfully target and defraud some TalkTalk account customers.

The breach has far–reaching implications for organisations and businesses and is set to increase the powers of the Information Commissioner's Office (ICO) in regulating the storage and use of personally identifiable information. This includes CCTV images and data from other electronic surveillance and security systems.

In this paper we discuss the breach, the subsequent parliamentary investigation and the changes to the regulatory framework that are likely to result.

The scrutiny of a parliamentary investigation

The October 2015 data security breach at TalkTalk is actually one of the few recent cases where the chief executive of a major corporate business has been seen to sincerely eat humble pie in public. Many who saw the broadcast interviews with TalkTalk boss Dido Harding would have been struck by the genuine contrition she projected.

Some might say that the heartfelt nature of this response reflected the seriousness of the breach; however, others may go a step further and say that it wasn't just the serious nature of the breach, but that Dido Harding understood TalkTalk had failed to put appropriate measures in place to adequately protect customer information.

To get closer to the truth and learn the lessons, a parliamentary report by the Culture, Media and Sport Select Committee has reviewed the circumstances surrounding the breach. It has made recommendations intended to strengthen the regulatory framework and increase the compliance burden. Essentially, as a direct result of the breach, the ICO is very likely to get sharper teeth in the shape of tougher enforcement actions.

Culture, Media and Sport Select Committee recommendations

The report, *'Cyber Security: Protection of Personal Data Online' contains 'Conclusions and recommendations'* that seem set to boost the ICO's ability to ensure personally identifiable information is stored and used in line with the Data Protection Act (DPA). The main points include:

Increased ICO resources

- Point 1 highlights a shortage of resource at the ICO to deal with the volume of cases and incidences of public concern. In response the ICO may increase staffing levels.

Escalating fines

- Point 5 suggests fines may be structured to reflect the overall approach and effectiveness of an organisation's IT security. For example, being breached by a 'plain vanilla' SQL injection attack, which is a well-known vulnerability for which adequate security should be in place, would carry a heavier fine than a breach that occurred because of a less well known vulnerability.

Informing of breaches

- Point 11 recommends the ICO should take a hand in publishing further guidance on informing the relevant authorities and those affected by security breaches. This supports the European Union General Data Protection Regulation (EU GDPR) in requiring the wider dissemination of breach information. The democratic will expressed through the 'Brexit' vote is unlikely to stop the UK legislature from implementing regulatory standards that make sense, even if the originate from Brussels.

Delaying and failure to report

- Point 12 suggests fines should be applicable in cases of delayed reporting of breaches and for failing altogether to report breaches. These should follow a sliding scale escalating in severity to reflect the seriousness of the incident.

Custodial sentences

- In point 13 the parliamentary committee report explicitly supports the ICO's call to bring into force Sections 77 and 78 of the Criminal Justice and Immigration Act 2008, which would allow a maximum custodial sentence of two years for those convicted of unlawfully obtaining and selling personal data.

Audit and reporting

- Point 14 provides highly detailed recommendations on how companies and other organisations need to demonstrate how much they spend on improving security and that they are spending it effectively. This includes reporting annually to the ICO on:

  i. Staff cyber-awareness training

  ii. When their security processes were last audited, by whom and to what standard(s)

  iii. Whether they have an incident management plan in place and when it was last tested

  iv. What guidance and channels they provide to current and prospective customers and suppliers on how to check that communications from them are genuine

  v. The number of enquiries they process from customers to verify authenticity of communications

  vi. The number of attacks of which they are aware and whether any were successful (i.e. actual breaches)

Traffic light system

- Point 15 stresses the parliamentary committee's support for the ICO's plan to create a privacy seal. This would be awarded to those which demonstrate good privacy practice and high data protection compliance standards. The initiative should also incorporate a traffic light system to help consumers understand which companies are compliant, which are making progress, and which have yet to take the issue seriously.

Governance, the organisation and cyber security

Additionally the report examined the issue of cyber security where it intersects with governance and the responsibility of those within the wider organisation.

'TalkTalk cyber-attack and response' is section 2 of the report. In point 15 it refers to the inquiry's view of how TalkTalk Board members' took responsibility for cyber security and data breaches.

When providing oral evidence to the select committee, Dido Harding confirmed that she saw herself as "accountable and responsible". She also explained that line responsibility for keeping customer data safe is split across a number of teams:

Security team

- Accountability for security policies, accountability for security audit, and accountability for security best practice, knowledge and dissemination within the organisation sits with the security function.

Technology team

- Implementation of systems and processes that comply with the policies sits with the technology function.

Operations team

- The implementation of the human elements of security—safe passwords, usage, complying with call centre policies—sits within the operations function.

Consequently, in a telecoms company, it is impossible to say that security only sits with the director of security. It is highly likely that this same situation exists in many medium and large enterprise organisations, regardless of the line of business or sector.

Responsibility and oversight

To help address the matter of governance, in point 16 of section 2, the report outlined an approach to help ensure cyber security is fully embraced within the broader governance mission of organisations facing similar challenges.

The report noted that while ultimate responsibility for cyber security within a company lies with the CEO, it would be highly unusual for the CEO of a company to resign over an attack.

It went on to emphasise that it is important that CEO responsibility is not used as a means to diffuse or avoid responsibility elsewhere. The day to day responsibility in any company should therefore be clearly allocated to a specific person, for example, the Chief Information Officer or the Head of Security.

To clarify matters here, the select committee makes these observations:

- It is appropriate for the CEO to lead a crisis response, should a major attack arise
- Cyber security should sit with someone able to take full day-to-day responsibility
- Board oversight should be applied to this responsible person who can be fully sanctioned if the company has not taken sufficient steps to protect itself from a cyber-attack
- To ensure this issue receives sufficient CEO attention before a crisis strikes, a portion of CEO compensation should be linked to effective cyber security, in a way to be decided by the Board

SUMMARY

Help to keep up with the increasing regulatory burden from iC2

iC2 is a leading mid-market security systems provider and was established in 2001. The business is owned and managed by a team with a collective experience of over 100 years in the electronic security business. iC2 holds CCTV and security accreditations with NSI and BSI.

Whatever regulatory changes result from the parliamentary report, iC2 offers a complete compliance service tailored to the size and needs of each client, which helps keep up to date with the increasing regulatory burden.

iC2 CCTV and surveillance compliance services help:

- Smaller businesses to meet their obligations while avoiding unnecessary cost and complexity
- Larger businesses to take complete control by understanding and meeting the compliance requirement in full

A prestigious client list including luxury international boutique brands, top flight sporting venues, retail developments and educational and social environments demonstrates how solutions are deployed to meet a variety of requirements.

From deterring theft of high value luxury goods, to sports fan and public safety and child protection, solutions are deployed to meet a range legitimate purposes for which they are appropriate and fit for purpose.

REFERENCES AND FURTHER READING

Cyber Security: Protection of Personal Data Online
UK Parliament; 20 June 2016
http://www.publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/14802.htm

In the picture: A data protection code of practice for surveillance cameras and personal information
ICO; CCTV Code of Practice; 2014
https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

Q&A guide: CCTV code of practice and Data Protection Act compliance
iC2 CCTV and Security Specialists (UK) Ltd
www.ic2cctv.com/pdfs/iC2-ico-compliance-guide.pdf

Appropriate response: A guide to security system integration, monitoring and verification
iC2 CCTV and Security Specialists (UK) Ltd
www.ic2cctv.com/pdfs/iC2-integration-verification-guide.pdf

Surveillance Camera Code of Practice
Home Office; 2013
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

iC2 DESIGN INSTALL PROTECT

T: 020 3747 1800

E: info@ic2cctv.com

W: www.ic2cctv.com

About Us

Keeping you safe and secure at all times

iC2 provide you with innovative solutions tailored to you and your sector. We are London-based with a national team of surveyors and engineers that work closely with our clients throughout the UK and internationally.

Our unique consultative approach allows us to tailor bespoke systems to your individual requirements, ensuring that your operational requirements are met.

We appreciate the need to demonstrate the best value to you every time and as a technology-led company, you can expect our cutting-edge and ground-breaking approach to serve your needs for many years to come.

Please feel free to contact us to discuss any requirements you may have. We are happy to give you impartial advice, should you have any queries.