



CCTV, the IoT & GDPR


Andrew Charlesworth

Reader in IT Law, University of Bristol

CCTV



- Estimated 5.9 million CCTV cameras in the UK
- The unofficial face of unaccountable surveillance overreach and invasion of privacy
- Popular perception of a lack of transparency and public engagement
- Significant 'legacy' equipment base
- Wide range of technology (analog, digital, infra-red, facial recognition, gait recognition)
- Wide range of users (home, private sector, public sector)



“It can be appropriate to disclose surveillance information to a law enforcement agency when the purpose of the system is to prevent and detect crime, but inappropriate to place them on the internet in most situations.”

UK Information Commissioner

Virgin Trains faces probe over whether release of Jeremy Corbyn CCTV broke law

The railway company released video and still images from one of its trains to show there were empty seats after Mr Corbyn complained of overcrowding.

The Independent (24/08/2016)


IoT

- IP cameras – inexpensive, flexible
 - backup output to local or cloud storage
 - accessible to users over the internet
 - live stream output for off-site monitoring
 - record/stream on varying environmental triggers

BUT

- Potentially vulnerable
 - unauthorised access to output
 - ability to disable cameras remotely
 - co-option into 'botnets' for DDoS attacks
 - compromise of connected computer networks.



An abstract graphic at the top of the slide features a series of overlapping, wavy bands of color. From left to right, the colors transition from a warm orange-red to a bright yellow, then to a vibrant green, and finally to a cool cyan-blue. These bands curve and flow across the top of the frame, set against a solid black background.

"In a relatively short time we've taken a system built to resist destruction by nuclear weapons and made it vulnerable to toasters."

Jeff Jarmoc, Head of Security, Salesforce

... or cameras.

DATA PROTECTION



- Case C-212/13 *Ryneš* (2014), CJEU.
 - Video surveillance that covers, even partially, a public space does not fall within the exemption for domestic use.
- *Woolley v Akbar* (2017), Scotland.
 - Failure to register
 - Failure to provide information
 - Failure to respect data subject rights
 - Failure to respect purpose and use limitation
 - Data kept for longer than necessary
 - £17, 000 in compensation to data subjects.

GDPR

- Industry & large users: Opportunity or burden?
 - Greater demonstrable accountability
 - CCTV specifically targeted by GDPR, esp. in public spaces and by public authorities
 - Privacy by Design/PIAs/DPOs
 - Cloud and IoT security risks
- BUT
 - Ability to develop sectoral Codes of Practice
 - Ability to develop sectoral Certification
 - Justification for technology spend
 - Driver for technology innovation.



GDPR

- Small scale users
 - Domestic exemption or data controller?
 - If data controller, then:
 - Hardware and software security – pressure on IoT hardware suppliers and cloud services to supply secured and securable technology - certification
 - Guidance for non-business users – clearly pitched and easily accessible.
 - Advice on good practice – signage, documentation, access, storage etc.
 - Practicalities – insurance coverage for non-compliance/ breach



PRIVACY FLAG

- Protecting and involving data subjects
 - Privacy Certification Scheme - designed to address emerging technologies, such as Internet of Things deployments.
 - Potential for public engagement in the context of Smart Cities, both with public administration legacy CCTV systems that are cloud-enabled, and with future IoT-based CCTV systems.
 - Future could see citizens able, via the web to:
 - identify ownership of particular CCTV systems
 - access information about purpose, storage, 3rd party access
 - request and receive access to their data.





University of
BRISTOL

<http://www.bris.ac.uk/law>



PRIVACY FLAG

<http://privacyflag.eu/>

 Cloudview[®]

<http://www.cloudview.co/>