Oireachtas Library & Research Service
Seirbhís Leabharlainne & Taighde an Oireachtais
Houses of the Oireachtas
Tithe an Oireachtais

L&RS Note

Data Privacy and Community CCTV Schemes

Roni Buckley, Parliamentary Researcher, Law

08 January 2019

Abstract

The aim of this Note is to establish if the crime prevention and detection purposes purported to be achieved by community Closed Circuit TV (CCTV) is proportionate to the potential privacy intrusion it poses. The introduction of smart CCTV schemes in a number of locations in Ireland in conjunction with the rollout of the General Data Protection Regulation (GDPR), throws into question the legitimacy and proportionality of advanced CCTV schemes.

Contents

Legal Disclaimer

Glossary

Glossary	
ANPR	Automatic Number Plate Recognition
CCTV	Closed Circuit TV.
Court of Justice of the European Union (CJEU)	The CJEU interprets EU law to make sure it is applied in the same way in all EU countries, and settles legal disputes between national governments and EU institutions. It can also, in certain circumstances, be used by individuals, companies or organisations to take action against an EU institution, if they feel it has somehow infringed their rights.
European Convention on Human Rights (ECHR)	ECHR is an international treaty to protect human rights and political freedoms in Europe. All Council of Europe member states have signed up to the European Convention on Human Rights.
European Court of Human Rights (ECtHR)	ECtHR is the judicial organ established in 1959 that is charged with supervising the enforcement of the European Convention on Human Rights.
GDPR	General Data Protection Regulation.
Hearsay	Evidence of a fact not perceived by a witness with his own senses, but asserted by him to have been stated by another person.
Inculpatory	To imply guilt.
Public interest privilege	This is privilege claimed by the State. In some very limited circumstances, the State may refuse to disclose information or documents in order to protect the public interest. In a particular defamation case, the Supreme Court held that to order discovery of a Garda file, assembled in an investigation of an abduction and murder which was still a live investigation, would be contrary to the public interest: *McDonald v RTE [2001 SC]* 2 ILRM 1; [2001 SC] 1 IR 355.
Surveillance	Systematic ongoing collection, collation, and analysis of data and the timely dissemination of information to those who need to know so that action can be taken.
Tort	A tort is a civil wrong which arises from a breach of a duty imposed by law, the main remedy for which is an action for damages. The principal torts are trespass, nuisance, defamation and negligence.

Summary

This Note examines privacy issues that potentially arise as a result of the installation of community CCTV schemes in Ireland. It does so by firstly examining the main reason for its utilisation: crime prevention and detection, and whether this aim is effectively achieved. Research from the UK into its effectiveness has been mixed, indicating its usefulness when detecting and solving certain crimes. However, the research equally shows how it has been ineffective in preventing other crimes. In Ireland few studies have been conducted into the effectiveness of CCTV in preventing crime. One doctoral study from 2012, however, showed inconclusive results on its effectiveness whereby some categories of crime reduced in CCTV operated areas, but equally increased in other areas.[1] Irish case-law indicates that CCTV footage is considered significant evidence in a criminal trial once its authenticity and reliability are established. While reference to CCTV footage as evidence in Irish jurisprudence is sparse, it is clear that it is useful for the investigation and prosecution of criminal offences.

Community based CCTV scheme is a Government initiative intended to support local communities who wish to install and maintain CCTV security systems in their area, with the aim of increasing public safety and to deter illegal or anti-social behaviour. This Note does not examine CCTV that is used for private, domestic purposes or CCTV used for private commercial reasons.

The Note discusses what the concept of privacy entails. In particular it considers the definitions of privacy as an unenumerated right in the Constitution, within case-law and various Review Group's working definitions. The Note goes on to consider the increasing sophistication[2] of surveillance cameras along with intentions by the Garda Síochána to increase data sharing, including CCTV footage. Surveillance cameras now have the ability to detect number plates as well as facial recognition and shape biometrics. In conjunction, the Garda Modernisation Programme has expressed intentions to significantly enhance data sharing, including CCTV data, as a part of their renewed investigations management system. The expansion, sophistication and increased sharing of CCTV data pose difficult questions for the legitimacy and proportionality of such ventures.

A case study of Duleek, Co. Meath, where 11 cameras were recently installed, presents interesting questions in terms of the proportionality and justification of having a significant number of cameras in a small rural community. Comparative analysis with the town of Royston in the UK, where a lesser amount of cameras were deemed unlawful by the supervisory authority there, suggests a strong possibility that Duleek's situation may be considered contrary to Data Protection requirements. The growing sophistication of cameras and their proliferation in small communities could potentially outweigh the crime prevention purposes for which they were installed.

The European Convention on Human Rights' (ECHR) Article 8 on privacy and the exceptions to it are also examined in some detail. Finally, it also looks at the recent Data Protection legislation and

[1] A. Donnelly, "To CCTV or not? An examination of Community Based CCTV in Ireland" (Dublin; DIT, 2012)
[2] See Garda Modernisation and Renewal Programme to introduce new and more advanced surveillance systems, discussed further on in the Note.

the General Data Protection Directive (GDPR) and how the obligations placed on data controllers to process data responsibly are relevant to CCTV surveillance.

Introduction

The increasing use and sophistication of CCTV cameras in Ireland could have society-wide implications given the potential for them to go beyond the limits of their legislative basis and of what privacy laws permit. Community CCTV cameras are described by the Department of Justice and Equality as aiming to:[3]

> *"Enhance existing policing provision within the community, to assist in the prevention and reduction of local crime, disorder and anti-social activity and to increase community involvement in the provision of legitimate, integrated responses to prevent and reduce crime in local areas in association with appropriate agencies"*

Section 38 of the *Garda Síochána Act 2005* sets out that the installation of community CCTV should be for the:

> *"Sole or primary purpose of securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences"*

The community CCTV scheme aims to build on the previous Department-funded community-based CCTV scheme which was launched in 2005 and operated by Pobal; it provided financial assistance to qualifying local organisations towards meeting the capital costs associated with the establishment of local community CCTV systems. Under that scheme, approximately €3.96 million was allocated to fund the 45 Community Schemes with the last of the funding being paid in July 2013.[4]

ECtHR and CJEU

To date the European courts have shown a lack of tolerance for CCTV surveillance that is not proportionate; they also illustrate how easily privacy laws can be breached. On the other hand, they show tolerance for surveillance which is legitimised by law and is premised on the aim of deterring and investigating crime. The GDPR, which came into force on 25th May 2018, could pose challenges for data controllers who must justify the legitimacy of CCTV schemes where it is argued that they are invasive and excessive.

The central question that arises, and which is examined in this Note, is whether the crime deterrence and detection achieved by CCTV schemes can be proportionately balanced with the potentially significant infringements they pose to personal privacy.

---

[3] *Infra.*
[4] Department of Justice and Equality, "Tánaiste announces new grant aid scheme for community-based CCTV systems" (April 2017).

The Concept of Privacy

Privacy is considered a fundamental human right that extends to all persons, no matter what their status. It can be broken down into a number of different rights including:

- A right to freedom from disturbance or attention;
- A right to control of personal information;
- The right to personal autonomy;
- The right to be protected from interference with physical or mental integrity.

Ultimately, it is the concept that individuals have a reasonable expectation to freedom from unwarranted attention. According to the Law Reform Commission privacy can be categorised into four forms:

1. Territorial privacy;
2. Privacy of the person;
3. Informational privacy;
4. Freedom from surveillance and interception of communications.[5]

Defining Privacy

The Working Group on Privacy was appointed by the Government in 2005.[6] It was set up in response to the duties imposed on the State under Articles 8 and 10 of the European Convention on Human Rights and in consideration of the principles stated by the European Court on Human Rights on the entitlements to privacy and freedom of expression, as well as consideration of the right to privacy under the Constitution. In its report the Group was tasked with considering and putting forward recommendations on a general tort of privacy and prescribing remedies and sanctions for breaches of invasion of privacy. The Working Group provided the following definition of privacy:[7]

> *"The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information".*

The Law Reform Commission Report on Privacy set out that:[8]

> *"Privacy as a concept includes a wide range of personal interests or claims which place limits on the right of society and of its members to acquire knowledge of, and to take action regarding, another person. At its core lies the desire of the individual to maintain control over information, possessions and conduct of a personal kind, and…to deny or control access thereto by others."*[1]

[5] Law Reform Commission, *Privacy: Surveillance and the Interception of Communications* LRC 57-1998, para. 1.13-1.14.
[6] "Report of the Working Group on Privacy" (31 March 2006).
[7] *Ibid*.
[8] Law Reform Commission, note 5.

In Ireland the right to privacy is an amalgam of several rights. These rights are embedded in our Constitution, the European Convention on Human Rights (ECHR), the EU Charter of Fundamental Rights and Freedoms (the Charter) and case law.[9]

Ireland and the Right to Privacy

The Irish Constitution

The Constitution does not contain a specific right to privacy; it is an unenumerated right embedded within it. It can be drawn from a number of different Articles, including:

- The right to private property (Article 43);
- Protection of family life (Article 41);
- The inviolability of the dwelling (Article 40.6.1˚);
- Personal autonomy (Article 40.3.1˚ and Article 40.3.2˚);
- Respect for human dignity (Preamble);
- Privacy of the ballot (Article 16.1.4˚);
- Litigation privacy (Article 34);
- The right to form associations and unions (Article 40.6.1˚).

Constitutional privacy has also been accepted by the Irish courts, where it has been well established that citizens have the right to be left alone by the State. In *Kennedy v Ireland*[10] Justice Hamilton held that the right to privacy was one of the unenumerated rights recognised in Article 40.3. Similarly in *Haughey v Moriarty*[11] Justice Hamilton stated that there was *"…no doubt but that the plaintiffs enjoy a Constitutional right to privacy".*

The Constitutional right to privacy is not absolute however. Its exercise is tempered by the Constitutional rights of others, the requirements of public order, public morality and the common good.[12] In *National Irish Bank v RTE*[13] Justice Lynch recognised there is also *"a public interest in defeating wrong doing and where the publication of confidential information may be of assistance in defeating wrong doing then the public interest in such publication may outweigh the public interest in the maintenance of confidentiality".*

[9] D. Kelleher, *Privacy and Data Protection Law in Ireland* (Bloomsbury, 2015) p. 5.
[10] *Kennedy and Arnold v Attorney General* [1987] IR 587 p. 592.
[11] *Haughey v Moriarty* [1999] 3 IR 1.
[12] *Cogley and others v RTE* [2005] 2 ILRM at 529; *Bailey v Flood* (14 April 2000) SC; *Haughey v Moriarty* [1999) 3 IR 1.
[13] *National Irish Bank v RTE* [1998] 2 IR 465.

Privacy as a Statutory Right

There is no defined statutory provision in Ireland which seeks to regulate for a general right to privacy. Instead there are a number of legislative provisions which create various privacy rights.[14] The *Data Protection Act 1988* (as amended by the *Data Protection (Amendment) Act 2003* and *Data Protection Act 2018*) affords individuals protection with regard to personal information maintained about them. The Act regulates the collection, processing, maintaining and disclosure of personal data (the Act will be discussed in greater detail below). It confers on individuals the right to establish that information exists about them and the right of access to such material. It also provides offences for the unauthorised disclosure of personal data. The 2003 Act extends the data subject's rights to include access, rectification and the right to object to processing where it would likely cause damage or distress. It also extends the responsibilities of the data controller and gives the Data Commissioner enhanced powers. Where a breach does occur the data subject is entitled to compensation under those Acts. The Data Protection Acts therefore provide a legal remedy for the invasion of some of the interests reflected in privacy.[15] However, the Acts are not intended to protect privacy *per se*; instead they regulate the processing of data. Individuals who have their privacy breached by being watched, listened to or discussed by third parties do not have recourse under the Acts if that information is not processed.[16]

A Tort of Privacy

It is well established that there is no general common law tort of breach of privacy.[17] In 2005 the then Minister for Justice rejected moves to establish such a tort, instead recommending reliance on "a case-by-case build-up of jurisprudence".[18] However, in 2006 a Privacy Bill was introduced to the Oireachtas. Section 2(1) set out that:

> *"A person who, wilfully and without lawful authority, violates the privacy of an individual commits a tort"*

The tort of violation of privacy was to be actionable without proof of special damage. Individuals were entitled to a level of privacy which was considered reasonable in all the circumstances having regard to the rights of others and to the requirements of public order, public morality and the common good.[19] Amongst a list of situations where a person was to be entitled to privacy, section 3(2)(a) highlighted the right to privacy from surveillance. However section 5(1)(d) provided a defence against a claim in a situation where the installation of a closed circuit television system

---

[14] Section 10(1) *Non Fatal Offences Against the Person Act 1997* creates an offence of harassment where a person intentionally interferes with another's privacy; section 114 *Copyright and Related Rights Act 2000* creates a right to privacy in certain photographs and films; section 4(3) *Mental Health Act 2001* requires that the treatment of people is carried out with respect to their privacy; requests for information under the *Freedom of Information Act 2014* can be refused where they would involve the disclosure of personal information; privacy of adoption records is guaranteed under the *Adoption Act 2010*. For a more extensive list please see The Working Group on Privacy, note 62, pp. 18-20.

[15] Working Group on Privacy, note 6, p. 23.

[16] *Ibid,* at 24.

[17] Kelleher, note 9, p. 51.

[18] Minister McDowell, Seanad Éireann 9 February 2005 at http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/takes/seanad2005020900005?opendocument

[19] Section 3(1).

was for a purpose authorised by law, or for the purpose of detecting or preventing the commission of an offence or the protection of persons or property. The Bill lapsed with the fall of the 30th Dáil. In 2012 Senators David Norris, Sean D. Barrett and Feargal Quinn introduced a Private Member's Bill, the *Privacy Bill 2012*, which aimed to provide for a new tort of violation of privacy, taking into account the jurisprudence of the Irish courts and the European Court of Human Rights. Section 2 of the Bill, once again, provided that it is a tort for a person to, wilfully and without lawful authority, violate the privacy of an individual. The tort was intended to be actionable without proof of special damage. Section 5 of the Bill provided a defence for the installation and operation of a closed circuit television system for a purpose authorised by law or for the protection of persons or property, for the prevention or investigation of crime, or under the law. However, this Bill also lapsed with the dissolution of the Dáil and the Seanad.

According to the Working Group on Privacy the principle torts of relevance, for a breach of privacy, are those of **trespass**, **nuisance** and the equitable action for **breach of confidence**.[20] While each has a role in supporting the enforcement of elements of personal privacy, none provides a complete workable remedy.

- The tort of trespass[21] is limited to unlawful incursions on land; it does not extend to surveillance activities that fall outside the boundaries of an individual's property.[22] In the case of *Lord Bernstein v Skyviews and General Ltd*[23] no remedy of trespass was available to a person whose private home had been photographed from an aeroplane passing over the airspace of his land. Therefore the tort is of limited use in providing protection of privacy interests.

- The tort of nuisance is also limited in its application. It has not been successfully applied to tortious claims for interferences with peace or well-being that did not have a basis in proprietary interests.[24] Two decisions, relating to the same proceedings, *Sullivan v Boylan (No.1)*[25] and *Sullivan v Boylan (No. 2)*[26] addressed aspects of tort law. The case involved menacing behaviour by a debt collector who was seeking payment of a contested bill for building work carried out on the plaintiff's home. The behaviour included parking outside the house in a van with 'Licensed Debt Collector' clearly on display. In his judgment Justice Hogan recognised that the tort of nuisance is only concerned with protecting proprietary interests rather than privacy interests. He added *"the fact that there is no statutory right to recover damages for this wrong [harassment] simply underscores the basic ineffectiveness of traditional tort law fully to vindicate the constitutional rights to the protection of the person"*.[27]

[20] Working Group on Privacy, note 6, p. 25.
[21] Tort of trespass provides actionable relief against unlawful incursions on private land.
[22] Law Reform Commission, *Consultation Paper on Privacy: Surveillance and Interception of Communications* (1998) para. 4.4-4.5.
[23] [1978] QB 479.
[24] Working Group on Privacy, note 6, p. 26.
[25] [2012] IEHC 389.
[26] [2013] IEHC 104.
[27] *Sullivan v Boylan,* note 25 & 26.

- The equitable action for breach of confidence only affords protection to confidential information and is dependent on the existence of circumstances which give a reasonable expectation of confidence. It does not generate a general entitlement to protect against disclosure of information. The duty of confidence was defined by Goff LJ in *Attorney General v Guardian Newspaper Ltd (No. 2)*[28] as:

> *"a duty of confidence arises when confidential information comes to the knowledge of a person…in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others."*

[28] [1990] 1 AC 109.

Video Surveillance

The development, digitalisation and miniaturisation of technology, as well as the expansion of surveillance provide opportunity for greater and more invasive monitoring of citizens. Camera surveillance is more frequently being sought for protection purposes, without necessarily considering the relevant prerequisites and arrangements.[29] According to the Article 29 Data Protection Working Party, this is because of the psychological effect video surveillance can have, whereby it is considered by the general public as an invaluable tool for detection purposes.[30]

Video Surveillance for Crime Prevention Purposes

Political support for CCTV installation has been consistently strong in Ireland. Former Minister for Justice, Michael McDowell TD is quoted as saying *"CCTV has proved extremely successful in the prevention and detection of crime and is part of a series of measures aimed at tackling street assaults, public disorder and fear of crime"*.[31] Most recently, Minister for Justice and Equality, Charlie Flanagan TD speaking in the Seanad, commented that:[32]

> *"The investment represented by the community-based CCTV grant-aid scheme reflects the value that communities, especially rural communities, place on CCTV as a means of deterring crime and assisting in the detection of offenders. I am conscious too that An Garda Síochána have reviewed the effectiveness of CCTV systems and indicated that it utilises CCTV in almost every criminal investigation, during major public events and sporting occasions, in the investigation of road traffic incidents and in many other areas requiring police action. Community-based CCTV systems have therefore proven to be of significant assistance in the prevention and detection of crime throughout the State."*

Under the Department of Justice and Equality General Conditions[33] the staff of the Grantor (Department of Justice and Equality and its agents) may undertake site visits and the grantee must adhere to the project being monitored by the Gardaí; the Gardaí will also need to be given access to the premises and records for that purpose.[34] Apart from the Department and its agents only persons authorised by the data controller will be given access to the media storage devices used in the CCTV system.[35] Access to the recorded CCTV images should be restricted by the data

---

[29] Article 29 Data Protection Working Party, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance* (Brussels, 2004).
[30] This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy.
[31] Appelbe, D., *CCTV as a crime prevention strategy: a review of the literature* (Centre for Criminal Justice and Human Rights, University College Cork, 2008).
[32] Merrion Street News, *Minister Flanagan encourages communities to apply for CCTV funding* (Merrion street, 2018).
[33] Department of Justice and Equality, "General Conditions for Grant Aid and Certificate of Acceptance Community Based CCTV Scheme".
[34] *Ibid,* para.6.
[35] Department of Justice Code of practice, note 50, para.4.3.

controller to a designated person or persons who have been Garda vetted. Other persons should not be allowed to have access to that area when a viewing is taking place.[36]

To date 35 Garda CCTV schemes are in operation which comprises in excess of 500 cameras. There are 45 community based CCTV schemes which involve 367 cameras and finally there are 1,031 designated safety camera zones across Ireland's road network as part of the Garda Safety Camera service.[37]

Table 1: Summary of surveillance cameras in operation in Ireland

Surveillance Type	Number of Schemes	Number of cameras
Garda CCTV	35 schemes	<500 cameras
Community CCTV	45 Schemes	367 cameras
Designated safety camera zones		1,031 cameras

Source: Merrion Street News, *Minister Flanagan encourages communities to apply for CCTV funding* (Merrion street, 2018). Compiled by L&RS.

Processing of CCTV Footage

In terms of **processing** a number of requirements are set out by the Department of Justice and Equality in their Code of Practice, some of which are set out here:

- All tapes must be stored in a lock-fast facility to which access is restricted, except when it is requested by the Garda authorities or during a judicial process;
- Only those authorised by the data controller shall have access to the tapes;
- Images should not be retained for longer than necessary by the data controller, the period stipulated by the Code of Practice is 31 days;
- Copies of tapes should not be made by the community based group. Only the data controller will make copies where the incident recorded is of a serious nature, where it is formally requested by the Gardaí, it is required in a trial, the DPP requests it or a data subject makes an access request;
- Under section 4.11 of the Code of Practice the use of automatic facial recognition technology is prohibited, in light of data protection requirements.[38]

The Department of Justice and Equality guidelines designate the **key objectives** of the scheme as the following:

- To enhance existing policing provision within the community;
- To assist in the prevention and reduction of local crime;
- Increase community involvement in the provision of legitimate responses to local crime;
- To facilitate the detection and investigation of crimes;

[36] *Ibid*, para.4.4.
[37] *Ibid.*
[38] Department of Justice and Equality, Code of Practice, note 50.

- To reduce the fear of crime; and to,
- Assist in the possible prosecution of offenders.[39]

Upon approval of the grant, the applicant will receive an up-front payment of 50% of the grant with the balance to be paid when the system is fully operational. The proliferation of video surveillance in Ireland under such schemes reflects the reasoning discussed by the Working Party; that there is a psychological effect related to it, whereby CCTV is sometimes regarded by the public as an 'invaluable tool' for the detection of offences.[40]

In 2017, the then Minister for Justice and Equality, Frances Fitzgerald, announced a new grant aid scheme for community CCTV systems. The scheme aims to build on the previous Department-funded community-based CCTV scheme which was launched in 2005 and which funded the establishment of some 45 Community CCTV systems. The last of that funding was paid out in July 2013. The original scheme was led by the Department of Justice and Law Reform and administered by Pobal. The scheme was intended to support community-based organisations that wished to provide community CCTV systems, in order to deter illegal or anti-social behaviour in places to which the general public have routine access, such as residential communities, city and town centres.[41] Justice Minister Charlie Flanagan acknowledged that €1 million was secured in Budget 2017 for the purposes of the new scheme, adding that it was envisaged that a similar amount will be made available in 2018 and 2019. Since the introduction of the grant, 27 applications have been received and 20 grants have been approved, totalling more than €500,000.[42] According to the Department of Justice and Equality, the applications that were rejected were on the basis that they were incomplete; the applications were returned and the community groups were encouraged to provide the necessary information to qualify for the grant.[43]

Eligibility criteria for Community CCTV

Under the new scheme, eligible community groups are able to apply for grant-aid of up to 60% of the total capital cost of a proposed CCTV system, up to a maximum grant of €40,000. The scheme is not aimed at installing CCTV in commercial areas such as shopping centres, industrial estates or business parks; neither is it available to private interests such as clubs or individual groups in order to provide security for specific buildings or premises.[44] It is solely aimed at existing, not-for-profit organisations that are broadly representative of the community, such as, Area Partnership, Community Development Projects, Family resource centres, the Local Authority and Community Enterprise. In addition, community based not-for-profit consortiums of private and community interests may apply under the aegis of an existing lead organisation.[45] The community group is not required to show that there is a certain level of crime in the area to justify the installation of CCTV cameras; they are, however, required to demonstrate there is a need for them and the local Gardaí

[39] Department of Justice and Equality Guidelines, note 45.
[40] Article 29 Working Party, note 6, p.3.
[41] For more detail see: https://www.pobal.ie/FundingProgrammes/CCTV/Pages/default.aspx
[42] Dáil Éireann Debates (29 November 2018) "Closed Circuit Television Systems"
[43] Finn, C. "No one has taken up the offer of free CCTV cameras from the Government" *The Journal,* 8 October 2017.
[44] Department of Justice and Equality, *Community Based CCTV Scheme Guidelines for Application*, section 1.
[45] *Ibid.*

should also submit a form which assesses the need.[46] Access to the CCTV data should be restricted except when requested by the Gardaí and that request was authorised by a member not below the rank of Superintendent.[47] Access should also be permitted where it is requested through a judicial process.[48] The following are some of the conditions which must be met in the application for it to be successful:

Code of Practice for Installation of Community CCTV:

a) The lead group for all applications must be an existing, legally registered body;
b) It is the responsibility of the lead group to ensure that all uses of the system are appropriate and in the interest of the community;[49]
c) The proposal must be approved by the local Joint Policing Committee;
d) The support of the relevant Local Authority is required. The lead group must also accept acting as Data Controller, in writing, and should nominate a designated person to have responsibility for the operation of the CCTV system. It is the responsibility of the Data Controller to ensure they are appropriately trained;[50]
e) The applicants must have authorisation of the Commissioner of An Garda Síochána in accordance with section 38 (section 38 sets out the conditions that must be met for the Garda Commissioner to authorise CCTV for the purpose of public security) of the *Garda Síochána Act 2005*;
f) In addition the applicants must have the support of a range of local groups and organisations such as residents' groups, local development groups, local businesses and public bodies;
g) Confirmation must be provided which shows that the necessary planning permissions and wayleaves have been secured;
h) A steering committee must be set up to ensure community participation and involvement;[51]

They must be able to demonstrate that:

i) There is a need for the CCTV system;
j) That its deployment will not intrude on privacy or infringe an individual's civil liberties;
k) That they have the funds to sustain the project for a five year period.

Under the Department of Justice Guidelines it is considered that monitoring of the CCTV cameras will improve the usefulness of the scheme. The Community based organisation will consequently have to ensure that all persons operating the CCTV system are appropriately trained in the system's use and have an understanding of the restrictions and legal obligations imposed on them by the laws in the area. It is anticipated that the staffed monitoring of such schemes will not be possible in many cases and so the CCTV systems will require a secure data recording and storage facility in order to be eligible.[52]

[46] *Ibid,* p.7 & 13.
[47] Department of Justice and Equality, Code of Practice, note 50, p.4.
[48] *Ibid.*
[49] Department of Justice and Equality, *Code of Practice for Community-Based CCTV Systems* section 1.4.
[50] *Ibid.*
[51] *Ibid.*
[52] Department of Justice and Equality Guidelines, note 45.

Effectiveness of CCTV in Crime Prevention

Research into the effectiveness of CCTV in preventing and detecting crime has been mixed. Early studies in the UK indicate that it is useful at reducing robberies in London Underground stations[53] and at reducing thefts in car parks.[54] However more recent studies indicate that it has had little or no effect at reducing crime in residential areas.[55] A systematic review by Welsh and Farrington in 2008 of 41 studies conclude that CCTV is effective in preventing some crimes in certain circumstances (for example, reducing incidents of vehicle crimes in car parks) but has little or no effect on other crimes (for example city centre crimes).[56] In terms of CCTV surveillance aiding with the detection of crime there are mixed results. In 1998 a study showed that, two years after the installation of a CCTV scheme in one Scottish town, the proportion of crimes solved by the police rose from 50% to 58%.[57] In a 2017 study by Ashby it was found that CCTV is frequently used in British Transport Police investigations (BTP). Recordings were utilised in 14,478 BTP investigations including assault (3,363), vehicle thefts (2,378), sexual offence (562) and robberies (273).[58] The availability of CCTV was associated with the increased likelihood of offences being solved. Ashby also claimed that the apparent low usefulness of CCTV reported in previous studies was likely attributed to CCTV only being used infrequently and not always being available to investigators.[59]

In Ireland, a 2012 study by Donnelly examined the effectiveness of CCTV in preventing crime in four locations; the study did not list the locations but did indicate that they were geographically spread out across the country and included one small town, two medium sized towns and one city suburban area.[60] Crime data was collected pre and post installation in the areas where the cameras were located.[61] The results were inconclusive showing that some categories of crime decreased in one area but increased in another. Table 2, below, sets out the crime figures obtained from the research:

---

[53] B. Webb & G. Laycock, *Reducing Crime on the London Underground: an evaluation of three pilot projects* (London Home Office; Crime Prevention Unit Paper Series, 1992).
[54] B. Poyner & B. Webb, *Successful Crime Prevention Case Studies* (London; The Tavistock Institute of Human Relations, 1987) and N. Tilley, *Understanding car parks, crime and CCTV: evaluation lessons from safer cities* (London Home Office; Crime Prevention Unit Paper Series, 1992).
[55] M. Gill & A. Spriggs, *Assessing the impact of CCTV* (London Home Office; Home Office Research Study Series, 2005).
[56] B.C. Welsh & D.P. Farrington, "Effects of closed circuit television surveillance on crime" (2008) 4(17) *Campbell Systematic Reviews.*
[57] J. Ditton & E. Short, "Evaluating Scotland's first town centre CCTV scheme" in C. Norris, J. Moran & G. Armstrong ed. *Surveillance, closed circuit television and social control* (Aldershot: Ashgate, 1998) pp. 155-173.
[58] M. Ashby, "The Value of CCTV Surveillance Cameras as an Investigative Tool: Empirical Analysis" (2017) 23 *Eur J Crim Policy Res* 441.
[59] *Ibid.*
[60] Donnelly, *infra* note 62, p.27.
[61] A. Donnelly, "To CCTV or not? An examination of Community Based CCTV in Ireland" (Dublin; DIT, 2012).

Table 2: Comparison table of Crime Figures pre and post installation of CCTV

Crime Category	Location No. 1			Location No. 2			Location No. 3			Location No. 4		
	Installation		Percent	Installation		Percent	Installation		Percent	Installation		Percent
	pre-	(post-)	Increase/ decrease	pre-	(post-)	Increase/ decrease	pre-	(post-)	Increase/ decrease	pre-	(post-)	Increase/ decrease
Attempts / Threats to murder, assaults, harassments and related offences	10	(8)	-20.0%	70	(60)	-14.3%	74	(68)	-8.1%	391	(356)	-9.0%
Dangerous or negligent acts	4	(8)	+100%	62	(61)	-1.6%	58	(36)	-37.9%	307	(246)	-19.9%
Robbery, extortion and hijacking offences	0	(0)	0%	1	(2)	+100%	2	(2)	0%	85	(101)	+18.8%
Theft and related offences	21	(31)	+47.6%	147	(221)	+50.3%	134	(118)	-11.9%	1943	(1639)	-15.6%
Fraud, deception and related offences	0	(2)	N/A	21	(31)	+47.6%	23	(15)	-34.8%	76	(112)	+47.4%
Controlled drug offences	1	(4)	+300%	55	(35)	-36.4%	49	(35)	-28.6%	698	(644)	-7.7%
Weapons and explosives offences	1	(3)	+200%	6	(12)	+100%	9	(7)	-22.2%	82	(124)	+51.2%
Damage to property and to the environment	24	(5)	-79.2%	132	(117)	-11.4%	110	(117)	+6.4%	1070	(997)	-6.8%
Public order and other social code offences	28	(19)	-32.1%	198	(220)	+11.1%	164	(138)	-15.9%	924	(938)	+1.5%
Burglary and related offences	3	(5)	+66.6%	49	(35)	-28.6%	73	(59)	-19.2%	992	(1008)	+1.6%

Source: A. Donnelly, "To CCTV or not? An examination of Community Based CCTV in Ireland" (Dublin; DIT, 2012)

Examination of the table above shows contrasting results. 'Damage to property and to the environment' decreased in locations 1, 2 and 4 but increased in location 3. Similarly 'Public order and other social code offences' decreased by 32.1% in location 1 and by 15.9% in location 3 but increased by 11.1% in location 2 and 1.5% in location 4.

Effectiveness of CCTV in prosecuting crime

There are a sparse number of Irish cases which examine the use of CCTV in criminal prosecution. However, the case-law that does exist indicates that CCTV is considered by the courts to be significant evidence in a criminal trial once conditions confirming its authenticity are established. It also indicates that CCTV evidence in a criminal trial is privileged because of public interest and investigative privilege.[62]

In the 2016 case of *DPP v McD*[63] Gardaí arrested McD in a car park where a car had been set on fire. The Gardaí also received CCTV footage from the complex manager showing McD at the car when it was set on fire. The defendant made an inculpatory statement when told that under section 19 of the *Criminal Justice Act 1984* the court could draw inferences from his failure to give account for his presence at the crime scene. At the Circuit Court trial the defendant argued that the CCTV evidence should be excluded as hearsay because the State had not provided any evidence as to the operation of the CCTV system, for instance, whether or not it was automated or required human intervention. The trial judge accepted the arguments and McD was acquitted. The case was appealed to the Supreme Court by the DPP. Justice McKechnie, in his judgment, stated that

[62] See Glossary for definitions.
[63] [2016] 3 I.R. 123

the trial judge had been incorrect in excluding CCTV evidence from the trial. The Court went on to summarise the general law of CCTV evidence. Amongst other conditions it stated that:

- CCTV footage should be regarded as real evidence and not as hearsay;[64] evidence as to its operation and functionality is therefore not required to establish this;
- CCTV footage does not enjoy any evidential presumption,[65] nor should a court take judicial notice of it, rather, it must be proved in an appropriate manner and to the required standard;
- Its provenance and authenticity must be established;
- Objection to its admissibility may be taken on any sustainable ground, including those covered by the exclusionary rule;[66]
- As with any piece of admissible evidence, its weight, value and credibility are matters for the jury;
- Because of its potency, care must be exercised to ensure the overall integrity of such evidence.[67]

In effect, the court outlined that CCTV footage will be considered as real evidence in criminal trials but with a number of conditions in order to ensure it is relied on appropriately. Its admissibility as evidence will be determined on a case by case basis by considering a number of factors, such as its authenticity. It will be a matter for the jury to determine what level of weight should be assigned to it. Finally, the court warns that a level of caution should always be attached to CCTV; because they recognise the potency of CCTV footage, its authenticity should be without question.

In the case of *McLaughlin v Aviva Insurance (Europe) and the Commissioner of An Garda Síochána*[68] the plaintiff brought a civil action against Aviva Insurance that they indemnify him for loss caused by a fire on his premises. The defendant refused on the grounds that it believed the plaintiff was responsible for the fire. A Garda criminal investigation was instigated at the same time. The plaintiff sought discovery of certain items including CCTV footage. The Garda Commissioner brought a motion for an order that the items were protected by privilege and therefore discovery had to be refused. The High Court rejected their claim. The case was appealed to the Supreme Court where the Garda Commissioner argued that while there is a public interest in the proper administration of justice, this had to be weighed against the competing interest of in the detection, investigation and prosecution of offences. Justice Denham allowed the appeal and ordered that the material was privileged on the basis of public interest and investigative privilege and that discovery should not be permitted until a decision on whether or not to prosecute was taken.

[64] Hearsay is evidence of a fact not perceived by a witness with his own senses, but asserted by him to have been stated by another person; *what someone else has been heard to say*. Sourced from Murdoch's legal dictionary.
[65] A legal presumption that places an evidential burden on the opposing party to suggest that the presumed fact is not true; i.e., that requires him to adduce some tangible evidence that the presumption should not operate, before it will cease to do so. Sourced from Oxford University Press.
[66] The rule whereby otherwise admissible evidence is excluded because of the constitutional imperative of protecting the personal rights of the citizen as far as possible, e.g. evidence obtained pursuant to an invalid search warrant. Sourced from Murdoch's legal dictionary.
[67] *DPP V McD, ibid*, para. 65.
[68] [2011] IESC 42.

In the case of *Stirling v Judge Mary Collins & DPP*,[69] while monitoring a remote CCTV surveillance, a Garda noticed a group of young people kicking phone boxes and shop windows on Aston Quay. The youths were arrested and charged with criminal damage. There were no eye witnesses and so the State's case depended on the Guards evidence and the CCTV footage. However, the CCTV recordings were lost. The appellant argued that the case should not proceed as there was a real risk of an unfair trial by solely relying on the Garda's testimony. In the Supreme Court Justice MacMenamin ruled that the case should not proceed on the grounds of an unavoidable risk of an unfair trial without the video-footage to support what the Garda witnessed.

Increasing Sophistication of Video Surveillance

The Garda Modernisation and Renewal Programme[70] was published in 2016 and sets out a five year programme aimed at improving the professionalism of the force and modernising and renewing the organisation. Some of the initiatives include an Investigations Management System which will enable the electronic management and tracking of all tasks and information related to an investigation from crime scene to court. The system aims to standardise and digitise management of all investigations; providing investigators with a single view of different sources of data. The Property and Exhibits Management system will give investigators a single view of all property and exhibits in Garda custody relating to their investigation. It will also enable the recording, tracking and safe custody of such items. This will allow investigators to search for and have access to all Garda content including documents, CCTV, video and audio.[71]

This information can then be sent electronically to other criminal justice agencies such as the Director of Public Prosecutions. As a result of centrally storing CCTV and audio files, the Gardaí indicate an intention to employ advanced CCTV technology which can automatically analyse CCTV footage. This will include expansion of the Automatic Number Plate Recognition (ANPR)[72] technology within its squad cars and its integration into the centralised storage system.[73] Garda access to ANPR and CCTV data is being expanded by working with State and commercial organisations. Efforts are being made to liaise with the National Roads Authority, Port Authorities, local authorities and private car park operators to get access to data from their ANPR systems, as well as CCTV systems operating on the motorway network.[74] The Modernisation strategy also outlines intentions to use more advanced CCTV techniques to enhance community safety through the use of 'face in the crowd'[75] and 'shape in the crowd'[76] biometrics that will identify "key targets".[77]

---

[69] [2014] IESC 13.
[70] An Garda Síochána, *Garda Modernisation and Renewal Programme 2016-2021* (Garda Síochána, 2016).
[71] *Ibid.*
[72] ANPR is a camera system that reads vehicle number plates using optical character recognition technology. Simultaneously the technology checks the number plate against a database of "watch lists" such as stolen cars or untaxed cars.
[73] An Garda Síochána Renewal Programme, note 70, p. 41.
[74] An Garda Síochána Renewal Programme, note 70, p. 50.
[75] A recognition system advanced enough to sift through large crowds of people, none of whom are consciously facing CCTV cameras, to get results.
[76] This is a form of "soft" biometrics; information which does not explicitly identify a person, but narrows the range of possibilities. This could be height, size, gait or other features.
[77] An Garda Síochána Renewal Programme, note 70, p. 101.

Concerns for Data Privacy and Surveillance:

New "smart" CCTV camera schemes, which have the potential for facial recognition and ANPR, have been introduced in cities such as Limerick and Duleek in Co. Meath. Fourteen towns in Limerick[78] are set to introduce 44 smart CCTV cameras which will be linked with data from environmental and footfall sensors as well as number plate recognition.[79] As a result of these developments the Data Protection Commissioner has stated her intention to appoint a special investigation unit, later this year, to conduct a comprehensive nationwide investigation into such CCTV schemes. The Commissioner expressed concerns about the ability to protect individuals' rights, the evidence base behind them, as well as questions around their legality.[80] In November 2018 the Commissioner issued a statement on data protection and community based CCTV.[81] The statement provided an update on an ongoing inquiry into surveillance of citizens by the State for law enforcement purposes through the use of technologies such as CCTV, body worn cameras, automatic number plate recognition enabled systems and drones. A team of authorised officers are, at time of writing, carrying out audits on the use of these technologies by data controllers in compliance with the GDPR and the Law Enforcement Directive. Part of this audit includes examination of the deployment of community based CCTV systems and whether section 38 of the *Garda Síochána Act* is being fully complied with; meaning that they are examining that the schemes have been approved by the Garda Commissioner and the Data Controller obligations are being complied with by the local authorities. This will involve an examination of matters such as transparency (public signage), retention periods for recorded footage, security of systems, access to systems and logging, as well as cooperation with the Gardaí for copies of footage needed for the investigation of crime. As each local authority is a separate data controller the Commissioner must undertake 31 separate audits. There are therefore no plans by the Commissioner to produce a single national report; however they may publish a summary of common findings across all local authorities in the future.[82]

The above mentioned initiative in Limerick is part of an "integrated smart CCTV platform" in 14 towns, identified in figure 1 below:

[78] The towns are: Abbeyfeale; Adare; Askeaton; Caherconlish; Castleconnell; Cappamore; Croom; Foynes; Kilmallock; Murroe; Newcastle West; Pallasgreen; Patrickswell and Rathkeale.
[79] E. Edwards, "Data Protection Commissioner to investigate State CCTV schemes" *The Irish Times* (01 March 2018).
[80] *Ibid.*
[81] Data Protection Commissioner, "Data Protection and Community Based CCTV Schemes" (November 2018).
[82] *Ibid.*

Figure 1: Map of Limerick City and County Smart CCTV camera locations

Source: Limerick City and County Council, "44 high spec Smart CCTV cameras being installed in 14 County Limerick towns" (29 November 2017).

The scheme is promoted as aiming to improve emergency responses to accidents, aid with traffic management and help fight against illegal dumping.[83] It allows for remote access of the CCTV feed on smartphones enabling authorised users access to live footage. A number of 'tourism' cameras are also being installed to allow for live online streaming. The footage from these cameras will be monitored on a 24 hour basis seven days a week at Moyross Community Enterprise Centre. The centre in Moyross is being upgraded to accommodate the expansion of the scheme which will facilitate the recording of up to 500 CCTV cameras.[84]

Some of the various purposes of the CCTV cameras in Limerick, outlined above, are at odds with the established purpose of Community CCTV schemes under the 2005 Act (securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences) and could be considered to contravene section 2(c)(ii) of the *Data Protection Act 1998* (data cannot be used for purposes contrary to what they were originally obtained for). It also contravenes the Garda Síochána and Equality policy on CCTV community schemes which prohibits facial recognition technologies.[85]

[83] E. Edwards, "Limerick council taking legal advice on CCTV project" *The Irish Times* (26 February 2018) 4.
[84] Limerick City and County Council, "44 high spec Smart CCTV cameras being installed in 14 County Limerick towns" (29 November 2017).
[85] Garda Síochána, *Code of Practice for Community Based CCTV Systems* p. 6.

Duleek Case Study:

In July 2017 in Duleek, Co. Meath six dome cameras and five ANPR cameras with recording systems were installed and accessible by both Ashbourne and Duleek Garda stations.[86] Concerns have been expressed that such systems could be linked to databases and algorithms that allow for tracking the entire population.[87] Media reports suggest that the village's installation of such a disproportionate number of cameras is driven by a perceived threat of crime rather an actual threat. Duleek did see an increase in some types of crime during the recession. The number of recorded burglaries, for example, spiked from 49 in 2006 to 91 in 2011. However, those numbers are already falling; recorded burglaries in 2015 were already back to pre-recession levels at 46.[88]

UK Comparative:

In the town of Royston in Hertfordshire in the UK, five cameras monitoring traffic with ANPR technology were deemed unlawful and excessive by the Information Commissioner's Office (ICO)[89] in 2013. The police force was found to have failed to carry out any privacy impact checks to assess its potential impact on people's privacy. The ICO also stated that the dominant presence of cameras made it impossible for motorists to enter the town without being recorded.[90] In comparison to Duleek (where 11 cameras have been installed) it should be considered that the town of Royston has a considerably larger population, but a lesser amount of ANPR CCTV cameras were deemed unlawful and excessive by the supervisory authority.

Remedies for data breach:

Currently, if a data subject suffers a breach of their data protection rights they are only entitled to rectification, blocking or erasure under sections 6 and 7 of the *Data Protection Acts 1998 and 2003*. If the individual suffers damage they will need to apply to the courts to seek compensation. According to Dr McIntyre the experience in other countries is that manually controlled security cameras have often been used for voyeurism, following attractive women and peeping in windows. However, Irish law does not currently have a criminal offence to prosecute this type of abuse.[91] This places the individual in a very vulnerable position whereby they are exposed to potentially significant privacy abuses but with very limited remedies where a breach occurs.

Data Sharing and Governance Bill

In light of the intentions by the Gardaí to share greater amounts of data, attention should be afforded to the *Data Sharing and Governance Bill* which was published on 12 June 2018 and is currently at third stage before Seanad Éireann.[92] The purpose of the Bill is to provide for better sharing of data across government departments and agencies in order to reduce costs and

[86] E. Edwards & K. Harris, "Does Blanket CCTV Coverage really provide security" *The Irish Times* (16 November 2017) 6.
[87] *Ibid.*
[88] TJ McIntyre, "Duleek use of CCTV to fight crime based on flawed logic" *Irish Times,* 20 November 2017.
[89] The UK's privacy regulator.
[90] T. Espiner "Police number plate camera scheme broke law in Royston" *BBC News* (24 July 2013).
[91] TJ McIntyre, note 87.
[92] Current status of Bill, as of November 2018.

enhance customer service. Data sharing is defined in the Department of Public Expenditure and Reform's policy proposal as the exchange of structured data between two public service bodies in relation to a specific entity such as a person, business, property or event.[93] The process envisaged involves:

- A receiving body determining that there is a need for the data from the sending body in order to support or improve its business process, perform a statutory function or provide evidence to support policy evaluation;
- The receiving body must identify an existing legal basis for data sharing;
- Technical and legal details, such as data protection restrictions, must be agreed in writing; and,
- The receiving body will need to match the shared data with data it currently holds.[94]

In addition the Bill outlines the intention for mandatory privacy impact assessments (PIA) in order to protect the rights of individuals. The assessment is designed to identify and address the privacy issues of a particular sharing initiative. It should identify any potential privacy risks that might arise from a current or proposed action and then examine ways to mitigate or avoid those risks.[95] Under section 5 of the Bill a 'Lead Agency' must be established who will act as the main contact point within the data sharing arrangement, whereby data subjects can obtain information about data sharing. They will also have to ensure compliance with agreements and data protection principles.

In developing their Modernisation and Renewal Programme the Gardaí will have to consider the above requirements if/when the Bill is enacted. As the receiving body the Gardaí will have to ensure there is a legal basis for the sharing of such data or the sharing is to enable them to carry out a statutory function and the conditions set out above will have to be provided for.

[93] Department of Expenditure and Reform, *Data-Sharing and Governance Bill: Policy Proposals*, p. 2.
[94] *Ibid.*
[95] Draft General Scheme of the Data-Sharing and Governance Bill, Head 9.

Privacy and the ECHR/European Charter

European Convention on Human Rights (ECHR)

Ireland has been a signatory to the ECHR since 1953. The *European Convention on Human Rights Act 2003* brought the Convention into force in Ireland. Under the 2003 Act the courts are empowered to grant declarations of incompatibility where it is found that provisions of domestic statute are in breach of the Convention. This provision sets in motion a procedure which enables the Houses of the Oireachtas to consider the declaration and provides a mechanism for the payment of compensation to individuals who suffer a loss as a result of the legislation. The right to privacy is addressed under Article 8 which provides that:

> *"Everyone has the right to respect for his family and private life, his home and his correspondence."*

Exceptions to Right to Privacy

Article 8(2) provides for exceptions to the right to privacy:

> *"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security,* ***public safety*** *or the economic well being of the country, for the* ***prevention of disorder or crime****, for the protection of health of morals, or for the protection of the rights and freedoms of others."*

In his 2017 Review of the Law on Retention and Access to Communications Data, Justice Murray commented that an assessment by the European Courts of whether an infringement is necessary depends on its proportionality and whether it provides sufficient protection against arbitrariness.[96]

ECtHR case law

The case of *Malone v United Kingdom*[97] emphasised that the potentially harmful consequences of intercepted data being handed over to the police could only be considered necessary in a democratic society where it contained sufficient protections against abuse:

[96] J. Murray, *Review of the Law on the Retention of and Access to Communications Data* (Department of Justice and Equality, 2017) p. 85.
[97] (1985) 7 E.H.R.R. 14.

> *"The Court accepts, for example, the assertion in the Government's White Paper (at para. 21) that in Great Britain "the increase of crime, and particularly the growth of organised crime, the increasing sophistication of criminals and the ease and speed with which they can move about have made telephone interception an indispensable tool in the investigation and prevention of serious crime"…This being so, the resultant interference can only be regarded as "necessary in a democratic society" if the particular system of secret surveillance adopted contains adequate guarantees against abuse."*

In *Z v Finland*[98] the ECtHR accepted that *"the interests of a patient and the community as a whole in protecting the confidentiality of medical data may be outweighed by the interest in investigation and prosecution of crime…where such interests are shown to be of even greater importance."*

However, the European Court of Human Rights has also recognised that the development and sophistication of modern surveillance technology has the potential to be abused and that interception using secret surveillance should only be used sparingly and where duly justified:[99]

> *"A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary… for the safeguarding the democratic institutions [sic] and… for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal."*

Privacy in a Public Place

The principle of privacy is not limited to circumstances where a person is in a private place. In *Von Hannover v Germany*[100] the Court extended the remit of Article 8 to public places:

> *"The public does not have a legitimate interest in knowing where the applicant is and how she behaves generally in her private life even if she appears in places that cannot always be described as secluded and despite the fact that she is well known to the public…private life in the Court's view, includes a person's physical and psychological integrity…[t]here is…a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life."*

[98] (1998) 25 E.H.R.R. 371.
[99] Szabó and Vissy v. Hungary [2016] ECHR 579.
[100] (2005) 40 E.H.R.R. 1.

In the case of *Peck v United Kingdom*[101] the applicant, who was suffering from depression, was caught on CCTV camera attempting to commit suicide in a public place. The local authority that operated the CCTV system permitted the footage to be circulated by the media to demonstrate the effectiveness of CCTV in preventing harm and consequently images of the applicant were shown on national TV shows with viewership of 9.2 million.[102] The case was appealed to the European Court of Human Rights. The ECtHR found that, while the inference with private life was in accordance with the law,[103] it was the disclosure of the images to a number of media sources that constituted a breach. The images were not accompanied with sufficient safeguards and were inconsistent with the guarantees afforded under Article 8 for respect of the applicant's private life.[104] Although the incident occurred in a public place, what ensued was viewed as surpassing what the applicant could have foreseen and disclosure by the local authority represented a serious infringement to his private life. The court further held that because the applicant had no effective remedy available to him on foot of this infringement, it constituted a breach under Article 13 of the Convention.

In re JR38[105] CCTV images of the defendant, rioting in Northern Ireland, were published in newspapers as part of a police campaign to identify rioters and discourage any further sectarian disorder. The Supreme Court found that Article 8 of the ECHR was not engaged, but if it had, no interference would have been determined. The Court stated that the test of reasonable expectation was an objective test that is to be broadly applied. The test did not exclude other factors from consideration such as age, consent, context or what the publicised material was used for. When the authorities speak of a protected zone of interaction between persons, it does not refer to interaction in the form of a public riot. While the taking and use of a photograph of an individual in a public place came within the ambit of Article 8, the question was whether this right was removed by virtue of the activity that person engaged in because the person could not have a reasonable expectation of privacy in those circumstances. In this case he could not have a reasonable expectation that photographs of him taking part in the disorder, taken for the sole purpose of identifying him, would not be published. The Court found that the interference was justified in the case as the publication of the photographs was in pursuance of a legitimate aim, it was lawful and proportionate. The aim of the policing policy was to prevent crime, prosecute offenders and divert young people from criminal activity. Dealing with sectarian violence was a pressing police and community issue. It was therefore said to have struck a balance between the interests of the community and the rights of the individual.

The UK experience indicates that while surveillance is capturing more and more detail, this will continue to be acceptable once it is for the legitimate aim of crime prevention and proportionate to the risk of the threat posed. Where breaches of privacy arise it is generally in how the material is processed or handled after it is gathered. It also suggests that individuals cannot expect total

---

[101] [2003] ECHR 44.
[102] *Ibid,* par. 20.
[103] There was a legitimate interference with private life as it fell within the definitions of section 163 Criminal Justice and Public Order Act 1994 and section 111 Local Government Act 1972.
[104] [2003] Info. T.L.R. 221
[105] [2015] UKSC 42.

privacy in public places, particularly when considering the nature of the activity they are involved in.

Covert Surveillance and the ECtHR:

Other rulings from the ECtHR show that interference with private life through the use of covert surveillance is considered legitimate once certain conditions are met. These are: that it is in accordance with the law, it has a legitimate aim and reasonable steps are taken to protect the privacy of the individual monitored.

In PG & JH v United Kingdom[106] the applicants were suspected of an anticipated robbery. Acting on information that an armed robbery was planned by the first applicant and 'B', the responsible police officer applied for authorisation to install a covert listening device into B's flat. Conversations at the flat were monitored and recorded until the device was discovered and the premises were abandoned. Although no robbery took place the applicants were arrested and charged with conspiracy to rob. On legal advice, the applicants declined to comment and refused to provide speech samples for comparison with the recordings. The police then obtained authorisation, in accordance with guidelines, to install covert listening devices in the applicants' cells and to attach such devices to the officers who were to be present when the applicants were charged. Samples of the applicants' speech were recorded without their knowledge and sent to an expert for comparison with the voices recorded at the flat. The Court found that the surveillance was an interference with private life because it had no basis in law; the guidelines upon which it was sanctioned had no statutory authority and were not accessible to the general public. It was therefore considered a violation of the right to privacy under Article 8.

The Court added that because there are circumstances where people involve themselves in activities which might be recorded or reported in a public way, then reasonable expectation to privacy may not always be a conclusive factor. However, in the current case the recording and analysing of the applicants' voices was considered processing of personal data and without any express legal authority there was a clear interference with private life.

In Rotaru v Romania[107] the applicant complained of a violation of his right to respect of private life based on the use of a Romanian Intelligence Service file which contained information about a conviction for insulting behaviour he received as a student. At that time he had written two letters of protest against the abolition of freedom of expression when the communist regime was established in 1946. The Court held that the documents contained various pieces of information about the applicant's life, in particular his studies, his political activities and his criminal record, some of which had been gathered more than 50 years earlier. In the Court's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of 'private life' for the purposes of Article 8(1) of the Convention. Such intelligence activities therefore have to be subject to legal safeguards and adequate supervision in order to comply with Article 8 and in this instance they were considered to be in contravention.

[106] (44787/98) [2001] ECHR 546 (25 September 2001).
[107] (28341/95) ECHR 2000-V, IHRL 2923 (ECHR 2000).

In Friedl v Austria[108] the applicant was photographed by the police and his identity noted during a demonstration. No prosecution was brought. The Court held that there was no violation of Article 8, even though the taking and storing of personal data during a public incident was closely related to his private life, there was a legitimate aim for the prevention of crime and disorder. The retention of records relating to a criminal case can be considered necessary in a democratic society for the prevention of crime.

The case-law indicates a balancing between the right to private life and permitting interference where the aim is for the prevention and detection of crime. A right to privacy in a public place is accepted in limited circumstances and only where it does not go beyond what can be reasonably expected (it is reasonable for people to expect that they will be recorded when involved in certain activities such as a protest or at a sports event for example). It would appear that State surveillance will be accepted where it can be shown that, firstly, sufficient safeguards are in place, secondly, that adherence with Article 8 is evident and finally, a legitimate purpose is linked to a statutory authority. However, when that information is retained with other identifying factors and the material is disseminated without sufficient protection of the individual's identity, then a serious breach may be concluded.

Privacy and the EU Charter of Fundamental Rights

The Charter was not intended to create a new right but rather, to reaffirm existing rights such as those that resulted from the case-law of the Court of Justice of the European Communities (CJEU) and the European Court of Human Rights (ECtHR).[109] One such right is the right to "respect for private and family life" which appears in Article 7:

> *"Everyone has the right to respect of his of her private and family life, home and communications".*

Article 8 of the Charter provides a right to protection of data:

> *"1. Everyone has the right to the protection of personal data concerning him or her.*
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
> *3. Compliance with these rules shall be subject to control by an independent authority."*

[108] (1996) 21 E.H.R.R. 83.
[109] Kelleher, note 65, p. 47.

Data Protection Laws

Lawfulness of Processing

CCTV surveillance is legitimised under the section 5(1) of the *Data Protection Act 1998* where its purpose is for the prevention, detection and investigation of crimes.

> **Data Protection Act 1998**
>
> Section 5: Restriction of right of access
>
> 5.—(1) Section 4 [110] of this Act does not apply to personal data—
>
> (a) kept[111] for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders…

The *Garda Síochána Act 2005* sets out the legislative basis for which CCTV systems can be installed by Gardaí and community groups. Section 38(1) outlines that:

> *"The Garda Commissioner may authorise installation and operation of CCTV for the sole or primary purpose of securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences".*

Authorisation to install CCTV can be given by the Garda Commissioner to any of the following under section 38(3) of the Act:

a) Members of the Garda Síochána;
b) Persons who meet the established criteria[112] and who are retained under a contract with the Garda Commissioner;
c) Persons who meet the established criteria and whose application for authorisation in respect of a specified area within the administrative area of a local authority has been approved by the local authority after consulting with the joint policing committee for that administrative area.

According to the Data Protection Commissioner, however, the data controller would need to establish a recurring breach of security to warrant constant electronic surveillance.[113]

Where equipment is installed either by private of public bodies, especially local authorities, for the purpose of security or detecting, preventing and controlling crime; the Article 29 Working Party[114] warns that there is a risk of blurring roles and responsibilities with regard to the task to be carried

[110] Section 4 of the 1998 Act refers to the right of access of a data subject to personal data relating to them.
[111] Kept by a data controller.
[112] See section on eligibility criteria for community CCTV discussed earlier in this Note.
[113] Data Protection Commissioner, *Data Protection and You* at https://www.dataprotection.ie/docs/Data-Protection-CCTV/242.htm .
[114] Article 29 Working Party, note 4.

out by the data controller.[115] Local authorities do not have direct competence over public order or public security matters. This function can only be carried out by law enforcement agencies.[116]

Data Protection Act 1988

Images captured by CCTV cameras are personal data and therefore subject to the requirements of the Data Protection Acts. The data controller (in the case of community CCTV schemes this would be the Local Authority)[117] would need to justify the obtaining and use of personal data by means of a CCTV system.

Proportionality

Under the Data Protection Acts the installation of such systems must be proportionate to the required need.[118] This means that CCTV surveillance is only proportionate when other preventive and/or security measures which do not require image acquisition (e.g. alarm systems, stronger street lighting) are clearly insufficient to achieve this aim. The same principle also applies to the selection of the technology. For instance, video surveillance may be proportionate where repeated assaults occur in one area, but not if it is a once-off occurrence. It must also be considered if video surveillance will actually work as an effective deterrent or simply re-locate the crime to another area.

Article 29 of the EU Directive on the protection of individuals with regard to the processing of personal data and on the free establishes a "Working Party on the Protection of Individuals with regard to the processing of Personal Data", generally known as the "Article 29 Working Party". It is made up of a representative from the data protection authority of each EU Member State (including the Irish Data Protection Commissioner), the European Data Protection Supervisor and the EU Commission. The Working Party is independent and acts in an advisory capacity. The Working Party seeks to harmonise the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics. The Working Party points out the following considerations for the purpose of proportionality when processing personal data by means of video surveillance:

- The visual angle of the camera: if the surveillance is to be performed in a public place the angle should not edge onto private property;
- Consideration of the type of equipment used: whether it is fixed or mobile;
- Installation arrangements: location of the camera;
- The possibility of zooming in and the possibility of blurring or deleting images from the footage;
- Image freezing functions;
- Whether there is a connection with a 'centre' to send sound or visual alerts;
- The steps taken on foot of the video surveillance: shutting down of entrances, calling up surveillance staff etc.[119]

[115] *Ibid,* p. 14.
[116] *Ibid,* p. 17.
[117] See section 1.4 of Garda Síochána "Code of Practice for Community Based CCTV Systems"
[118] Section (2)(1)(c)(ii) requires that data collected are "adequate, relevant and not excessive".
[119] Article 29 Working Party, note 4 pp. 19-20.

Other considerations that the data controller will have to keep in mind are the retention period for footage and images resulting from video surveillance. Under the Community CCTV Code of Practice it is recommended at 31 days. The Working Party suggests that an exception to short retention periods would be cases where an alert has been issued or a request has been made deserving specific attention whereby the data controller should await the decision of either the police or judicial authorities.[120] Consideration will also have to be attributed to cases where the identification of a person is easily made by associating images of the person's face with other identifying information about their conduct or activities. Finally, the Working Party advises that attention should be afforded to any decisions to communicate surveillance data to a third party. Such communication should not occur where the entities involved are unrelated to the video surveillance.[121]

General Data Protection Regulation

The GDPR replaces the Data Protection Directive 95/46/EC and is designed to harmonise data privacy laws across Europe and to protect all EU citizens from privacy and data breaches in a world that is vastly more technologically advanced than when the 1995 Directive was introduced. It also aims to reshape the way organisations across the region approach data privacy.

The collection of images through the medium of video surveillance is a form of processing and therefore must comply with data protection legislation. With the GDPR coming into force on May 25th 2018, CCTV systems will need to be operate in accordance with the principles set out below:

> **Purpose-** images and recordings should only be collected through CCTV for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The purpose of the CCTV must be underpinned by one of the legal justifications set out under Article 6[122] and the images should be processed lawfully, fairly and in a transparent manner. CCTV surveillance is legitimised under Article 2(2)(d) where it is for "the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security". Local authorities will therefore need to justify why more advanced camera technology is required for crime prevention and detection, so that it can be justified as proportionate and necessary.
>
> **Retention and storage-** recordings and images must be adequate, relevant and limited to what is necessary. Data may only be stored for longer periods where they are for archival, historical or scientific research purposes (Article 5). Retaining CCTV data beyond a

[120] Article 29 Working Party, note 4 p. 20.
[121] Article 29 Working Party, note 4 p. 21.
[122] Some of the legal justifications include:

- Where the data subject has given consent;
- Where it is necessary for the performance of a contract;
- Where it is necessary for compliance with a legal obligation;
- Where it is necessary for the purposes of the legitimate interest pursued by the controller.

reasonable time period would need to be justified and according to the Data Protection Commissioner should be regularly purged where it is no longer necessary.[123]

Integrity and confidentiality- appropriate technical and organisational security measures must be used to keep CCTV images and recordings secure against unauthorised or unlawful disclosure (Article 5). This is an issue which Local Authorities and Community Groups will need to be cognisant of when installing CCTV cameras under the scheme.

Penalties- data controllers (in the case of Community CCTV this is the local authority) should be aware that the GDPR has increased fines to a maximum of 4% of annual global turnover or €20 million (whichever is greater) where they are in breach of the different obligations[124] set out in the Regulation (Article 83).

Consent- the conditions for consent have been strengthened and the request for consent must be given in an intelligible and easily accessible manner, with the purposes of processing attached. It must also be as easy to withdraw consent as it was to give it (Article 7). Consent may cause concern as it would not be practical to expect all members of the community to provide it before installation of the CCTV scheme, withdrawal of consent is also something that would be virtually impossible to guarantee.

Data Subject Rights- have been strengthened considerably.

i. Breach notification will become mandatory in all Member States where a breach is likely to result in a risk to the rights and freedoms of the individual. Data subjects will need to be informed within 72 hours (Article 34).
ii. Data subjects will have a right to access whereby they can obtain from a data controller confirmation as to whether or not personal data is being processed about them and for what purpose (Article 15). Any person whose image is recorded on a CCTV will therefore have the right to seek and be supplied with a copy of their personal data from the footage. The data should be provided in electronic format. Where images of individuals appear on the footage that are not that of the requesting party, the onus is on the data controller to pixelate or mask the identity of that individual before supplying the footage to the requestor.[125]
iii. Under the right to be forgotten data subjects have the right to request a data controller to erase his/her personal data, to cease further dissemination of it and have third parties stop processing it. This right is tempered by the data controller's obligation to compare the subject's right with the public interest in the availability of the data, when they are considering such requests (Chapter 3, Section 3).

Facilities will need to be established by the local authority which ensure data subjects are notified of any breach of their rights and are granted access where any images/video of them are being processed as well as erasure of their data where requested.

[123] Data Protection Commissioner at https://www.dataprotection.ie/docs/Data-Protection-Rule-7/31.htm
[124] The obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; the obligations of the certification body pursuant to Articles 42 and 43; the obligations of the monitoring body pursuant to Article 41(4).
[125] O'Flynn Exhams Solicitors, *CCTV and GDPR* at http://www.ofx.ie/cctv-and-gdpr/

Privacy by design- while already a well developed concept, is now a legal requirement under the GDPR. It requires that data protection is a central feature from the onset of designing a new system (Article 25). Data controllers are required to only hold and process data which is absolutely necessary for the completion of its duties (Article 5). The location of cameras will therefore be a key consideration because use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy will be difficult to justify.

Data Protection Officers (DPO)- DPO appointment will be a mandatory requirement under the GDPR for controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences (Article 37). Local authorities will need to appoint a DPO because CCTV cameras do entail systematic monitoring on a large scale.

While the implementation of community CCTV schemes is legitimised under Article 2(2)(d) and can be legislated for by Member States under Article 23, the sophistication of the technology could potentially pose a number of risks and put into question the proportionality of its use.

Conclusion

Privacy is a fundamental right strongly embedded in our Constitution as well as international conventions to which we are bound. It therefore demands a high level of protection and safeguarding. However it is not an absolute right and must be balanced with the obligation on the State to ensure public safety and maintenance of public order through interferences with privacy which are solely aimed at preventing, investigating and deterring crime. Surveillance through CCTV cameras is justified under this obligation and supported by legislative basis in Ireland. Privacy in a public place is recognised by the ECtHR as being limited to a reasonable expectation of privacy. The same Courts have equally permitted interference with the right to privacy by public authorities through the use of covert surveillance for crime prevention and investigation purposes. Breaches of Article 8 are more likely to be associated with how the footage/images are utilised or processed and whether there are sufficient safeguards in place during the processing to protect the data subject's identity. Based on this information it is likely that community CCTV schemes will be considered legitimate under Article 8 once they are not used beyond the purpose of crime prevention and the data accumulated is processed appropriately and safely.

The new data protection provisions will place more burdensome obligations on local authorities to ensure that CCTV data is appropriately collected, processed, retained and deleted. It will also assign stronger rights to data subjects wishing to access their data. Delineations between the role of the local authority and the Guards in terms of law enforcement functions should also be clarified when setting up such schemes. CCTV schemes such as those in Duleek and Limerick will need to show that other forms of crime control that are less intrusive were not sufficient in order for the number of cameras installed to be justified; especially when most recent crime statistics suggest a decline with only 46 burglaries recorded in 2015 compared to 91 in 2011. Such schemes will need to identify an actual risk of crime rather than a perceived risk.

Although academic research has provided little clarity on the effectiveness of CCTV, it is now, unquestionably a normalised function of public order control throughout Irish society. Focus would advisably be placed on examining any potential breaches of data protection arising from the interlinking of surveillance systems (as anticipated in the Garda modernisation scheme) and whether or not the quantity and sophistication of the cameras used is proportionate to the objective of crime prevention in the designated area.

Contact:
Houses of the Oireachtas
Leinster House
Kildare Street
Dublin 2
D02 XR20

www.oireachtas.ie
Tel: +353 (0)1 6183000 or 076 1001700
Twitter: @OireachtasNews

Library & Research Service
http://library
Tel: +353 (0)1 6184701
Email: library.and.research@oireachtas.ie

Connect with us