THE CRIMINAL JUSTICE (SURVEILLANCE) ACT 2009: AN EXAMINATION OF THE COMPATABILITY OF THE NEW ACT WITH ARTICLE 8 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS

John Barry *

ABSTRACT

Prior to the enactment of the Criminal Justice (Surveillance) Act 2009, there was no law in this State regulating the power of the Gardai to conduct covert surveillance. Gardai nevertheless undertook this type of surveillance and used the intelligence gained to assist in the investigation of serious crimes. The enactment of the 2009 Act aims to bring the law on covert surveillance in Ireland into line with that of many European countries. Notwithstanding this fact, there are some parts of the 2009 Act that require detailed analysis in order determine its compatibility with article 8 of the European Convention on Human Rights (ECHR). The European Court of Human Rights (ECtHR) has been to the forefront in ensuring that surveillance law in European Union states meets certain key standards. These standards such as accessibility and foreseeability are addressed in detail in this paper in order to determine whether the new Act will pass these judicial tests. Key issues such as the lack of judicial control in issuing authorisations, the failure to define some of the main terms such as State Security in the Act and the level of judicial oversight envisaged in the new Act are all examined in this paper. These issues are analysed in detail and tested against the case law of the ECtHR in order to see if the new Act complies with some of the keys decisions of the ECtHR on covert surveillance.

A INTRODUCTION

The term covert surveillance covers a wide variety of surveillance techniques from intercepting phone calls to physically following suspects and monitoring their movements. Modern surveillance techniques utilise various types of electronic surveillance technology. Initial research for this paper highlighted the fact that there was no law governing the activities of Gardaí undertaking certain types of surveillance. Gardaí could intercept phone calls and postal communications under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993 (hereinafter the 1993 Act) but there was no legislation governing electronic surveillance such as covert listening devices, tracking devices and covert cameras. The Garda National Surveillance Unit (NSU) has been in operation for many years using modern technology to monitor the activities of suspects. Perhaps one of the reasons the activities of the NSU do not receive widespread attention is that they have not used the material from their surveillance activities in direct evidence. For example, if the Gardaí secretly monitored a conversation in a pub, they would use this information to aid a certain investigation but they would not use the actual recording as evidence in a criminal trial.

The European Court of Human Rights (ECtHR) has been a key proponent of change in the area of surveillance law with particular reference to article 8 of the European Convention on Human Rights (ECHR).

[1] Irish law has to be compatible with the ECHR following the enactment of the European Convention on Human Rights Act, 2003.[2] An Garda Síochána undertakes surveillance in this country to combat serious crime, drug trafficking and terrorist activity. Despite the fact that there was no law in this jurisdiction governing certain types of surveillance, the Irish State has not been before the ECtHR to justify this apparent legal vacuum in Irish surveillance law. Notwithstanding that the Law Reform Commission had produced a report on this matter in 1998,[3] it was events on the streets of Limerick, particularly the murder of Shane Geoghegan that focused the mind of the current government and led to the enactment of the Criminal Justice (Surveillance) Act, 2009 (hereinafter the 2009 Act). The jurisprudence of the ECtHR in relation to the interception of communications and covert listening and monitoring brought to the fore some potential legal deficiencies in Irish surveillance law notwithstanding the introduction of the 2009 Act. The definitions of some of the key terms in the Act are analysed and tested against the jurisprudence of the ECtHR. The absence of judicial oversight is an issue in certain sections of the 2009 Act. Crucially, the question of who is looking after the interests of the citizen in light of these new surveillance powers requires in-depth analysis.

Article 8 of the ECHR guarantees a person's right to respect for his family and private life[4] and outlines how public authorities may only interfere with this right in specific circumstances. Any interference must be in accordance with the law and necessary in a democratic society in order to protect such interests as national security, prevention of crime and public safety.[5] Article 8 has been used by many EU citizens to challenge the use of surveillance by member States to gather evidence against them. The ECtHR has examined the legality of surveillance carried out by various public authorities within member States of the European Union (EU). Irish citizens have been slow to challenge the legality of Garda surveillance in the ECtHR unlike citizens of other EU States who have successfully challenged the power of various public authorities to use surveillance to gather evidence. A detailed analysis of the judgments will show how the lack of appropriate law in many jurisdictions has resulted in breaches of article 8. The ECtHR has provided clear direction to member States on the quality of the domestic legislation that is required in order for member States to comply with article 8. In *Klass v Germany*,[6] the ECtHR established the right of a State to place its citizens under surveillance under certain specific situations. This case related to a number of lawyers and a Judge who claimed that a German law, known as the G10 Act,[7] dealing with the monitoring of post and telecommunications was in breach of the

---

* BBS (UL), Solicitor, LLM Criminal Justice (UCC).

[1] The European Convention on Human Rights (ECHR) sets forth a number of rights and freedoms such as the right to life and the right to a fair trial. State parties to the convention undertake to secure these rights to everyone within their jurisdiction. See *Convention for the Protection of Human Rights and Fundamental Freedoms, ETS.* See n 4-5 for full definition of Article 8 of the ECHR.

[2] The enactment of this Act obliged Ireland to adhere to the provisions of the European Convention on Human Rights.

[3] See Law Reform Commission LRC 57-1998 *Report on Privacy: Surveillance and the Interception of Communications* (Dublin Law Reform Commission 1998).

[4] Art 8(1) of the ECHR provides as follows; "Everyone has the right to respect for his private life, his home and his correspondence."

[5] Art 8(2) of the ECHR provides as follows; "There shall be no interference 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 or morals, or for the protection of the rights and freedoms of others."

[6] Series A No 28 (1978) 2 EHRR 214 PC.

[7] The applicants claimed that Art 10, para 2 of the Basic Law (Grundgesetz) and a statute enacted in pursuance of that provision, namely the Act of 13 August 1968 on Restrictions on the Secrecy of the Mail, Post and

ECHR. The Court accepted the locus standi of the applicants even though they were not able to show that they had been the subject of surveillance.[8] It found that the power to carry our surveillance lay under article 8(2),[9] with specific reference to a State's right to safeguard democratic institutions. The Court went on to highlight the danger of laws such as the G10 Act undermining democracy under the pretence of protecting it. The Court was not going to allow States to use whatever measures they wanted to counteract terrorism and espionage.[10] The Court required the surveillance to have adequate measures and protections against abuse. Each case was to be judged on its merits and the Court would look at such issues such as the grounds for ordering surveillance, the length and scope of the surveillance, the competence of those permitting, carrying out and supervising the surveillance measures and the remedies available at national law to those at whom the surveillance is directed.[11] In acknowledging the right of the German authorities to undertake surveillance, the Court sought to find a 'compromise' between the rights of the individual and the need to defend a democratic society.[12] In this case, the Court found that the G10 Act was not in breach of article 8.

B KEY PRINCIPLES UNDERLYING ARTICLE 8 OF THE ECHR

The Court has been particularly consistent in requiring that no laws breach the principles of *foreseeability* and *accessibility*. Foreseeability means that the law must be laid out in enough specific detail in order that individuals can regulate their conduct accordingly.[13] Accessibility refers to the fact that the law must be readily available to the public at large and not restricted to those who carry out the surveillance. The ECtHR has been consistent in its rulings in this area and States whose legislation breached these principles were found not to have complied with article 8 of the ECHR.

The general principles as to what constitutes 'in accordance with the law' under article 8(2) were set out in the case of *The Sunday Times v United Kingdom* (hereinafter the *Sunday Times* case).[14] The Court referred to three main principles. Firstly, the public authority must have a legal basis for their action(s). Secondly, citizens must have access to the law and this *accessibility* to the law must give them adequate guidance as to what circumstances are covered by the law.[15] Thirdly, the law must be constructed with sufficient clarity to allow the citizen to be able to reasonably foresee how this law will affect him or her should they act in a certain manner.[16] This concept of *foreseeability* does not have to be absolute but must be reasonable given the circumstances of the case. These principles were cited with approval in *Malone.*[17] In this case, the Court expanded on the principle of foreseeability in relation to the interception of communications, by stating that this does not mean that the individual under surveillance should be able to foresee when his

---

Telecommunications (Gesetz zur Bexchrankubg des Brief-, Post-underFernmeldegeheimisses) hereinafter referred to as the "G 10 Act" were contrary to the ECHR.

[8] *Klass v Germany* (n 6) para 41.

[9] ibid para 42.

[10] ibid para 49.

[11] *Klass v Germany* (n 6) para 50.

[12] ibid para 59.

[13] Covington & Burling 'Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention On Human Rights' [2003] <http://www.privacyinternational.org/countries/uk/surveillance/pi_data_retention_memo.pdf> 8 (5 February 2010).

[14] *The Sunday Times v United Kingdom* (1979-1980) 2 EHRR 245.

[15] ibid para 49.

[16] ibid.

[17] *Malone v United Kingdom* Series A 82 (1984) 7 EHRR 14 PC para 66.

communications are likely to be intercepted, as this would allow him to change his behaviour.[18] The Court reiterated that the law must be clear as to the 'circumstances' and 'conditions' under which public authorities can initiate 'this secret and potentially secret surveillance.'[19] The Court found that the British authorities were in breach of article 8 on the basis that the legal rules governing the interception of communications breached the principle of foreseeability as these rules were internal guidelines and not available to the public at large.[20] The Court also stated that since surveillance measures are by their nature not open to scrutiny by the public, the law must not be drafted in terms that gives the public authorities 'unfettered' power and discretion and therefore the law must be clear on the limits of any such discretion.[21] In seeking to find the protection available to the individual under the umbrella of 'in accordance with the law' the Court differed from the judgment in *Klass* where the Court in that case stated that the protection was to be under the confines of what is 'necessary in a democratic society' under article 8(2) of the ECHR.

Subsequent decisions in *Halford v United Kingdom*,[22] found that the absence of any domestic legislation clearly breached the principle of foreseeability since the interception of these communications had not been in accordance with the law and was in breach of article 8. Similarly in *Huvig v France,*[23] (hereinafter *Huvig*) which also dealt with the interception of telephone conversations, the Court again focused on the issue of foreseeability. The Court made the point that the law governing the monitoring of phone calls and other forms of communication had to be precise in order to keep pace with the increasingly sophisticated technology available to the authorities.[24] The French Government referred to the fact that they had in place a large number of safeguards to protect against arbitrary interceptions, some of which were expressly laid down in the French Code of Criminal Procedure and others stemming for Court judgments over the years.[25] However, in some cases, the safeguards were not clear and came from interpretations of the legislative provisions. It was not defined who could have their phone tapped nor the offences which would allow such tapping.[26] The Court was also not satisfied that the procedures for the creation, transmission, storage, and destruction of the intercepted conversations were sufficiently clear in French law.[27] The Court found that French law was lacking in the legal certainty required for it to be compatible with article 8 and thus found that the French authorities had breached this article.[28]

---

[18] ibid para 67.
[19] ibid.
[20] *Malone v United Kingdom* (n 17) para 68. This was an administrative practice, which covered how the police were to undertake surveillance. However, the internal guidelines governing this practice were not available to the public.
[21] ibid.
[22] (1997) III; 24 EHRR 523.
[23] (1990) 12 EHRR 528.
[24] ibid para 32.
[25] ibid para 32-33. The French Government listed seventeen protections which were provided for under French Law such as;-
- the need for an investigating Judge, that is an independent judicial authority, to authorise surveillance;
- the latter's supervision of senior police officers and the possible supervision of the Judge himself by the Indictment Division (chambre d'accusation) of the Court of Appeal;
- the exclusion of any subterfuge or ruse consisting not merely of telephone tapping but in an actual trick, trap or provocation;
- The duty to respect the confidentiality of relations between suspect or accused and lawyer.

[26] *Huvig v France* (n 23) para 87.
[27] ibid.
[28] ibid para 64.

C COVERT SURVEILLANCE PRIOR TO THE ENACTMENT OF THE 2009 ACT

Prior to the enactment of the 2009 Act there was no law governing the use of covert surveillance devices by Gardaí. In the absence of any law governing this type of activity, Gardaí were able to use such devices to gather intelligence. This intelligence, while not used as direct evidence in Court, was often nevertheless crucial in furthering criminal investigations. It could be argued that since there was no basis in law for the use of these surveillance devices, then any evidence that flowed from such use would have been not only breach of the rules of evidence but also breached article 8 of the ECHR. Whilst no Irish citizen challenged this legal vacuum, similar cases taken by individuals in other EU states provide us with an insight into how the ECtHR dealt with the absence of a legal basis for surveillance. In the case of *Khan v United Kingdom*[29] (hereinafter *Khan*) the applicant visited his friend's house in Sheffield, a Mr Bashforth. Sheffield police had installed a covert listening device in Bashforth's house under authorisation from the Chief Constable of South Yorkshire Police as they suspected he was dealing drugs and this was the only means by which they could get the necessary proof. The police had not expected that Mr Khan would visit Bashforth's house. As a result of the covert listening device, the police recorded a conversation between the two men during which the applicant admitted to being a party to the importation of drugs during the previous year. The applicant pleaded guilty once the trial judge had allowed the evidence of the recording in during the *voir dire* and he was sentenced to three years' imprisonment. His subsequent appeal went to the House of Lords, who accepted that the evidence was obtained in breach of article 8. Nevertheless, the House of Lords held that the evidence should not be excluded.

The matter came before the ECtHR. The applicant claimed that there was no statutory basis for the use of covert listening devices in the United Kingdom and that the recording of his conversations were not obtained 'in accordance with the law.'[30] The United Kingdom authorities accepted that the covert listening device did interfere with the applicant's private life protected under article 8 (1), but claimed that this interference was not in breach due to the fact that it was 'in accordance with the law and necessary in a democratic society to prevent crime.'[31] The authorities also claimed that foreseeability in the context of covert surveillance was different to other areas of law and did not breach the convention provided the scope of the discretion given to the authorities was clear and they referred the court to the Home Office Guidelines which were accessible to the public, though not on a statutory basis.[32] The court emphasised the need to have clear domestic law so that individuals could be aware of the circumstances in which the police could carry out covert surveillance.[33] The court did not accept that the Home Office Guidelines were accessible and made the point that they were not legally binding which meant that the police actions lacked any basis in domestic law. It was on these grounds that the court found the covert surveillance to be in breach of article 8.

The United Kingdom authorities were again before the ECtHR in the case of *PG & JH v The United Kingdom*.[34] The police were investigating the possibility of a robbery taking place involving the applicants and placed a covert surveillance device in the applicant's flat. In relation to the covert listening device, the court held, citing *Khan* that there was no

[29] 2000-V; 31 EHRR 1016.
[30] ibid para 23.
[31] ibid para 24.
[32] ibid para. 24.
[33] ibid para 26.
[34] 2001 – IX; 46 EHRR 51.

domestic law governing the use of such devices at the relevant time and so this action was not 'in accordance with the law' and a breach of article 8.[35] Prior to the enactment of the 2009 Act, there appears to have been no basis in Irish law for the use of covert surveillance devices. Therefore, intelligence obtained by the Gardaí using such equipment would have been in breach of the principles of foreseeability and accessibility as required by the ECHR.

D CLEARING THE HURDLES: THE 2009 ACT AND ARTICLE 8 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS

Having due regard to some of the key principles already discussed, the 2009 Act is a major development in the law in Ireland dealing with covert surveillance. The Act is arranged in 19 sections. The analysis of the Act will focus on some of the key provisions with some of the more contentious sections requiring more detailed attention. Section 1 defines the key terms in the Act. Surveillance is defined as monitoring, observing, listening to or making a recording of a particular person or group of persons or their movements, activities and communications, or (b) monitoring or making a recording of places or things by or with the assistance of surveillance devices. Surveillance device means an apparatus designed or adapted for use in surveillance but does not include binoculars, night vision equipment, CCTV, or cameras used in public.[36]

1 Cameras, Videoing and Surveillance

The exclusion of cameras from the definition of a surveillance device may come under judicial scrutiny particularly by the ECtHR. According to the Minister for Justice, Dermot Ahern, cameras were purposely excluded as they are used as part of regular day–to-day policing and the aim of this Act was to regulate electronic surveillance devices.[37] The Minister sought to make a distinction between the use of cameras for ordinary everyday policing and targeted surveillance.[38] This distinction between ordinary and targeted surveillance is somewhat difficult to reconcile with the definition of surveillance in that the repeated and targeted monitoring and recording of people using cameras would come seem to constitute surveillance. This is the viewpoint of the Irish Human Rights Commission (IHRC) who advocated the inclusion of cameras as a surveillance device.[39] In excluding cameras, the legislation attempts to allow Gardaí to continue using cameras as part of everyday surveillance as they currently do without bringing this type of surveillance within the remit of the Act. Minister Ahern has stated that he does not want to create a situation whereby Gardaí would have to apply for a surveillance warrant every time they intended using cameras or night vision goggles.[40] The current situation is that evidence relating to this type of monitoring by the Gardaí can be given as direct evidence in court. It is interesting to note

---

[35] ibid para 38.

[36] Under s 1(5) of the 2009 Act, surveillance device does not include (a) an apparatus designed to enhance visual acuity or night vision, to the extent to which it is not used to make a recording of any person who, or any place or thing that, is being monitored or observed, (b) a CCTV within the meaning of s 38 of the Garda Síochána Act, 2005, or (c) a camera, to the extent to which it is used to take photographs of any person who, or anything that, is in a place to which the public have access.

[37] 30 Dáil Debates (24 June 2009) 873.

[38] ibid.

[39] Irish Human Rights Commission *Observations on the Criminal Justice (Surveillance) Bill 2009* May 2009 6.

[40] 30 Dáil Debates (24 June 2009) (n 37) 873.

that the Law Reform Commission in a report published on this area in 1998 had recommended that cameras should be included in the definition of surveillance.[41]

In the context of the jurisprudence of the ECtHR, the use of cameras by the Gardaí could amount to interference under article 8.[42] One of the key issues is whether there is a permanent record of the material obtained and whether the authorities have identified individuals contained in these records.[43] In a situation where the Gardaí photograph suspects and then maintain these photos in a systematic manner, then this would seem to constitute an interference with the private life of the individual.[44] The European Commission for Human Rights in *Friedl v Austria*[45] examined a situation whereby Mr Friedl was photographed and recorded by video recorder during the course of a demonstration. The demonstrators had been informed prior to the action that they were in breach of Austrian law and had been asked to leave the area. However, the Austrian authorities argued that the police did not seek to establish the identities of the demonstrators who had been photographed nor did they enter the photographs into any data processing system.[46] The Austrian authorities paid compensation to Mr Friedl and destroyed the photograph. As a result, the Commission rejected a breach of article 8. However, this case occurred fourteen years ago and it remains to be seen how the ECtHR would deal with such an issue today.

In *Govell v United Kingdom*,[47] (hereinafter *Govell*), the applicant was subjected to police surveillance. However, in this case, the police used covert listening and camera equipment during the course of the investigation. The police drilled a hole into the applicant's living room from the house next door, which would have enabled someone to listen to the applicant from this house or to attach a listening device. The police also installed camera equipment in the property next door.[48] All these devices were installed under authorisation of the acting Chief Constable of West Yorkshire Police who submitted that these authorisations were issued under the appropriate Home Office Guidelines governing surveillance.[49] The applicant submitted that the surveillance was not 'in accordance with the law' as the Home Office Guidelines were not 'sufficiently accessible.'[50] The Commission noted that the UK authorities were in the process of drafting legislation to cover this type of surveillance.[51] However, this law, which would be known as the Police Act 1997, could not be applied to this case. The Commission referred to the fact that the applicant had difficulty obtaining the Home Office Guidelines, which in any case were not legally binding and for this reason ruled that, the law was not sufficiently clear and was in breach of article 8.[52] In this situation, the ECtHR clearly stated that covert surveillance equipment including cameras

---

[41] Law Reform Commission LRC 57-1998 *Report on Privacy: Surveillance and the Interception of Communications* (Dublin Law Reform Commission 1998) 130. Surveillance is defined as follows; - "surveillance" includes aural (hearing) and visual (optical) surveillance, *irrespective* (emphasis added by author) of the means employed.

[42] n 4-5 regarding the definition of Art 8.

[43] *PG & JH v United Kingdom* (n 34) paras 57-59.

[44] ibid para 57. Private life issues only arise when a permanent or systematic record comes into existence.

[45] Application no. 15225/89 26th January 1995.

[46] ibid para 8.

[47] Report of the European Commission of Human Rights 14th January 1998.

[48] Report of the European Commission of Human Rights (n 47) para 87.

[49] The Home Office Guidelines were guidelines put in place to cover the use of surveillance equipment by UK police during surveillance operations.

[50] In March 1994, the applicant had requested disclosure of the relevant Home Office Guidelines on the authorisation for surveillance. However, West Yorkshire Police Authority refused disclosure on the basis that the documents were covered by public Interest immunity. The applicant subsequently obtained a copy of these guidelines through other means.

[51] Report of the European Commission of Human Rights (n 47) para 59.

[52] ibid paras 62 - 63.

requires a basis in law to comply with article 8. In light of this decision, the exclusion of cameras from the 2009 Act may not comply with article 8 in this regard.

The question of whether the covert videoing of a suspect amounts to a breach of article 8 was examined in the case of *Perry v The United Kingdom*[53] (hereinafter *Perry*). Mr Perry was a suspect in a robbery. Perry failed to turn up for an identification parade and the police videoed him under authorisation while he was in a police custody area in order to get a picture of him to show to witnesses.[54] In order to get a clear picture of Perry, the police regulated the camera in order to get clear footage of him. The still of this footage was subsequently included in a photomontage, which was shown to witnesses. The video was also shown in Court during Perry's trial. The ECtHR ruled that whilst the accused would have expected and been aware that he was being filmed in the police station, the subsequent use of the footage went beyond the normal expected use of the camera. The fact that the footage was permanently stored and included in a montage constituted the processing and collecting of personal data about Mr Perry.[55] As a result, the Court ruled that there had been an interference with the applicant's right under article 8. The Court also ruled that this interference was not in accordance with the law, as the police had not complied with the code of practice in relation to the aspects of the video recording and were therefore in breach of article 8(2).[56]

In *Perry*, the ECtHR is making clear that where the material obtained from recordings or cameras is collected and stored for further use, then this would be interference under article 8 (1). This interference can only be justified under article 8 (2) if it is done in accordance with the law. For example if the Gardaí place a person under surveillance, photograph that individual, then process and store this material, then there would seem to be a clear interference with that individual's privacy. Therefore, in excluding the use of cameras from the 2009 Act, the government are not giving any basis in law as required by the ECtHR to justify the use of cameras during surveillance. The three principles espoused in the *Sunday Times*[57] case, namely that there be a legal basis for the action, coupled with accessibly and foreseeability would seem to be absent in this situation. Given that cameras are not included in the legislation, there does not seem to be any available guidelines or code of practice in operation governing what the Minister describes as ordinary surveillance in order to regulate the behaviour of Gardaí undertaking this type of surveillance. Irish citizens therefore cannot with any degree of certainty foresee when the Gardaí can use cameras to record them and their activities, which would seem to be a breach under article 8.

2 Grounds for Undertaking Surveillance

One of the key provisions of the Act relates to the application for authorisation for a surveillance warrant. Under section 4, a superior officer[58] of the Garda Síochána may apply to a judge of any District Court area for a surveillance warrant.[59] In order to obtain this

[53] (2004) 39 EHRR 76.
[54] ibid para 39.
[55] ibid para 41.
[56] ibid. para 47- 49.
[57] *Sunday Times v United Kingdom* (n14).
[58] Definition of a superior officer (n88).
[59] s 4(1): 'A superior officer of the Garda Síochána may apply to a judge for an authorisation where he or she has reasonable grounds for believing that – (a) as part of an operation or investigation being conducted by the Garda Síochána concerning an arrestable offence, the surveillance being sought to be authorised is necessary for the purposes of obtaining information as to whether the offence has been committed or as to the circumstances

warrant, the surveillance must relate to the investigation of an arrestable offence[60] or concerned with the security of the State[61]. The term security of the State, unlike the term arrestable offence is not defined in the legislation. Senator Ivana Bacik makes the point that surveillance and bugging has been authorised in Ireland in the past under the very vague heading of 'maintaining the security of the State.'[62] In *Kennedy,*[63] the Supreme Court could find no justification for the tapping of the applicant's phones. The fact that the intercepted transcripts were passed on to the then Justice Minister added a clear political dimension to the tapping. The ECtHR has stated that definitions within surveillance legislation must be sufficiently clear in order for the citizen to regulate their behaviour accordingly. In *Weber* & *Savaria v Germany*[64] (hereinafter *Weber*), the ECtHR found that the citizen could foresee the consequences of his actions, as the legislation was sufficiently precise and specified the situations in which surveillance could take place. These included such events as an armed attack on Germany, money laundering and arms trafficking.[65] This is important in the jurisprudence of the ECtHR in that the Court in this case was satisfied that German law complied with article 8 of the ECHR. It should be noted that the ECtHR ruled that the phrase 'national security' was too general a term.[66] Weber was a German national and Savaria was a Uruguayan national, both of whom lived in Montevideo, Uruguay. Weber worked as a freelance journalist for various German media outlets, where she investigated, among other things, arms trafficking. Savaria took messages for Weber while she was away working on assignments. The applicants submitted that the German Fight Against Crime Act 1994, which amended parts of the G10 Act,[67] breached their rights under article 8 and could possibly be used to place them under surveillance. It was their submission that technological progress made it possible to intercept their communications anywhere in the world using catchwords, which were secret.[68] The key issues, which the applicants complained of, related to the process of strategic monitoring of communications, the transmission of this data to the various relevant authorities and the use of it by them, the destruction of this data and finally the refusal to give notice on the restrictions on the secrecy of telecommunications.[69] The court here, as in many of the aforementioned cases, focused on the issue of foreseeability. The court observed that the G10 Act specified the category of offences, which allowed the

---

relating to the commission of the offence, or obtaining evidence for the purposes of proceedings in relation to the offence,

(b) the surveillance being sought is necessary for the purpose of preventing the commission of arrestable offences, or

(c) the surveillance being sought is necessary for the purpose of maintaining the security of the State.'

[60] Under s 2 (1) of the Criminal Law Act 1997, an arrestable offence means an offence for which a person of full capacity and not previously convicted may, under or by virtue of any enactment, be punished by imprisonment for a term of five years or by a more severe penalty an includes an attempt to commit any such offence.

[61] s 4(1) (n 59). See s 4(1) (c) dealing with security of the State.

[62] 23 Seanad Debates (2 July 2009) at 673. Senator Bacik refers specifically to the bugging of the phones of journalists Bruce Arnold and Geraldine Kennedy in 1983.

[63] *Kennedy v Ireland* [1987] IR 587.

[64] (2008) 46 EHRR SE5.

[65] *Weber* (n 64). A detailed list of events where surveillance is permitted is outlined in the German legislation.

[66] ibid para 64.

[67] G10 Act (n 8). In this situation, the applicants alleged that certain aspects of the Fight Against Crime Act 1994 which amended the G10 Act, disregarded their fundamental rights, notably the right to secrecy of communications (Art 10 of the Basic Law), the right to self determination in the sphere of information (Arts 2(1) and 1(1) of the Basic Law), freedom of the press (Art 5(1) of the Basic Law) and the right to effective recourse to the Courts (Art 19(4) of the Basic Law).

[68] The G10 Act allowed for the monitoring of wireless telecommunications, which could be transmitted via satellite, or radio relay links. Signals emitted from foreign countries are monitored from interception sites on German soil and the data collected is used by the German authorities.

[69] s 4(1) (n 61) para 74.

interception of communications, and these were detailed in section 3(1) of the G10 Act.[70] It also noted that the category of person who could have their communications monitored was specified under section 3(1) and (2) of the G10 Act. The person concerned had to have taken part in an international telephone conversation via satellite or radio and used certain key words linking them with the offences outlined above.[71] The court also set out the minimum standards relating to surveillance that should be set out in statute; namely the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephone tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or tapes destroyed.[72] Having examined these procedures in detail, the court was satisfied that the foreseeability element had been dealt with adequately by the German authorities and ruled that the amended G10 Act was not in breach of article 8.[73] This case highlighted the fact that terms such as 'security of the State' were too vague. The lack of a precise definition of such terms in the 2009 Act may bring it into conflict with article 8 of the ECtHR.

Similarly, the recent case of *Liberty and Others v The United Kingdom*[74] (hereinafter *Liberty*), is particularly relevant to the issue of covert surveillance and particularly the need to have precise definitions of key terms such as national security. In this case, the applicants, Liberty, British Irish Rights Watch, and the Irish Council for Civil Liberties alleged that the British Ministry of Defence (MOD) operated an Electronic Test Facility ("ETF") in Cheshire, which was built to intercept 10,000 simultaneous telephone channels coming from Dublin to London and on to the Continent.[75] Between 1990 and 1997, it was alleged that the ETF intercepted all telephone, facsimile and e-mail communications carried on microwave radio between two British Telecom radio stations in Wales and Cheshire. These links carried much of Ireland's Telecommunications traffic. The applicants were in regular telephone contact with each other during this time and would have passed on legal advice to people. They allege that much of their telecommunications traffic would have been intercepted by the ETF. The applicants alleged a breach of article 8 stating that this interception did not have a basis in law and was not accessible and foreseeable.[76] They also argued that the procedure for issuing warrants under the Interception of Communications Act 1985 (hereinafter the 1985 Act*)*, was unclear and the law did not specify how the authorities selected, disclosed, used, or retained the information intercepted.[77] This case, like *Weber*, involved what the court described as 'generalised strategic monitoring' or blanket monitoring of communications traffic as opposed to the targeting of specific individuals.[78] In other words, the authorities had systems in place such as 'catch words' which would trigger the surveillance. The court

[70] s 3(1) of the G10 Act states: 1. An armed attack on the Federal Republic of Germany. (FDR); 2. The commission of international terrorist attacks in the FDR; 3. International arms trafficking within the meaning of the Control of Weapons of War Act and prohibited external trade in goods, data processing programmes and technologies of considerable importance; 4. The illegal importation of drugs in substantial quantities into the territory of the FDR; 5.Counterfeiting of money committed abroad; 6. The laundering of money in the context of the Acts listed under points 3-5. Pursuant to s.3(1), third sentence, restrictions on the secrecy of telecommunications could also be ordered for telecommunications via fixed telephone lines and for mail in order to identify and avert the dangers listed in s.3(1), second sentence point 1.

[71] *Weber* (n 64) para 97.

[72] *Weber* (n 64) para 95.

[73] ibid para 102.

[74] (2009) 48 EHRR 1.

[75] ibid para 5.

[76] ibid para 45.

[77] ibid.

[78] ibid para 63.

in its judgment found that this blanket monitoring granted to the executive 'unfettered discretion'[79] as in theory everybody who received or sent communications within this time could have had their communications intercepted. The court also found that the 1985 Act was not specific as to what captured material was listened to or read. It found that such terms, as 'national security, and 'preventing and detecting serious crime' were too general.[80] In relation to the 'catch words' used, the British authorities had put in place 'arrangements' governing the selection of material for examination and for the dissemination and storage of intercepted material.[81] However, these arrangements were not made public and thus seemed to breach the principle of accessibility. The court then went on to cite with approval *Weber* where the German authorities considered it prudent to include detailed provisions relating to catch words.[82] The court also referred to the fact that the G10 Act set out clear and detailed rules regarding the storing, retention destruction and use of captured material.[83]

In an Irish context, the term security of the State could allow for the covert surveillance of persons or political groupings based on their political beliefs. It is interesting to note that during the Seanad debate on the legislation it was revealed that two members of the Houses of the Oireachtas had been under surveillance.[84] Independent TD for Mayo, Dr Jerry Crowley suspected that his phone was being tapped and asked the complaint's referee[85] to investigate the apparent official tapping of his telephone.[86] Deputy Crowley has been closely associated with the Shell to Sea campaign, which opposes the Corrib Gas pipeline plans in Co Mayo. The grounds for interceptions by the State under the 1993 Act are unclear to say the least. However, by not defining with sufficient clarity terms such as 'security of the State' in the 2009 Act, the potential for abuse becomes more likely. It would have been prudent to define this term in the legislation to ensure that citizens would know with sufficient clarity the types of actions that came under the umbrella of security of the State.

3 Judicial v Non – Judicial Authorisation of Surveillance

The question of the appropriate legal authority to issue a surveillance authorisation arises under section 5 of the 2009 Act. The legislation allows for a judge of any District Court area to issue an authorisation ex parte.[87] However, under section *7*(3) surveillance may be carried out in certain situations without judicial authorisation and a superior officer[88] may grant

---

[79] ibid para 64.
[80] ibid.
[81] *Liberty* (n 74) para 66.
[82] ibid para 68. The catchwords used by the German authorities had to be listed on the monitoring order. The catchwords also had to be related to one of the specific offences, which they were investigating. See note 123 for a complete list of authorised offences. In contrast, the United Kingdom legislation did not require the specific catchwords to be listed on the surveillance warrant.
[83] *Liberty* (n 74) para 68.
[84] 30 Dáil Debates (30 April 2009) 560. This fact was revealed by Deputy Aenghus Ó Snódaigh of Sinn Féin who told the Seanad that he was informed of this surveillance by a previous Minister for Justice, Equality, and Law Reform in response to a question as to whether any member of the Houses of the Oireachtas was under surveillance, electronic or otherwise.
[85] Under s 9(3) of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993 a person who believes that a communication sent by him has been intercepted can apply to the Referee for an investigation into the matter.
[86] See Digital Rights Ireland <http://www.digitalrights.ie/category/mass-surveillance/page/3/> (28 August 2009).
[87] See ss 5(1*)* (a) and (b*)* of the 2009 Act.
[88] Under s 1(a) of the 2009 Act 'superior officer' means in the case of An Garda Síochána, a member of An Garda Síochána not below the rank of superintendent.

approval for the surveillance under certain circumstances such as the suspect absconding, evidence being destroyed or if the security of the State is likely to be compromised.[89] This approval has to meet the same criteria that a judicial authorisation would have to meet under section 4 and lasts for a maximum period of 72 hours.[90] The power of senior Gardaí to issue warrants is available for offences under the Criminal Justice (Drug Trafficking) Act, 1996[91] and for certain offences under the Offences against the States Act, 1939.[92] However, under the 2009 Act, senior Garda officers can issue approval for surveillance for a wide variety of offences found under the umbrella of arrestable offences and this warrant can last for 72 hours. It is the nature of policing that warrants may be required at speed in certain situations. However, a period of 72 hours, which is three full days, would seem to be a generous time period without judicial oversight. It has been suggested that a period of 24 hours would allow all those involved to obtain judicial approval.[93] Each District Court area has a judge on call at weekends and over holiday periods to cover emergency court sittings in each district. It would therefore seem realistic that these judges could deal with any applications for surveillance warrants within 24 hours. The ECtHR makes it clear that they require a close level of judicial supervision of any warrants issued as was highlighted in a number of rulings by the ECtHR when it held that surveillance legislation lacked the appropriate judicial supervision and therefore breached article 8.

This requirement for judicial authorisation is made clear in some key decisions of the ECtHR. In *Kopp v Switzerland*,[94] (hereinafter *Kopp*) the applicant, who was a lawyer and a Swiss national, had his office phone lines monitored by the Swiss authorities in November and December 1989. The applicant's phone lines were monitored as a third party, by the authorities who were investigating the leaking of secret documents from a government department. The applicant alleged a violation of article 8 on the grounds that Swiss law prohibited the tapping of phones where the individual was a lawyer as these conversations are considered privileged.[95] The Swiss government claimed that his conversations as a lawyer were excluded and that only the conversations that related to matters not related to his profession were monitored. [96] The government explained that a specialist post office official undertook the decision as to what conversations were relevant.[97] The court emphasised the necessity of 'clear rules' again under the ambit of foreseeability and held that in this case the law was not sufficiently clear as to by whom, and under what grounds, the distinction between privileged and not privileged material was to be made.[98] The court was particularly concerned that an official of the postal service without supervision by an independent judge was assigned to adjudicate on what conversations were relevant.[99] In light of this fact, namely the lack of judicial oversight at this specific stage, the court found that there had been a breach of article 8.

---

[89] See ss 7(1) and 7(2) of the 2009 Act.
[90] See s 7(8) of the 2009 Act.
[91] s 8(1) of the Criminal Justice (Drug Trafficking) Act, 1996 amends s 26 of the Misuse of Drugs Act, 1977 so as to allow a member of An Garda Síochána not below the rank of Superintendent to issue search warrant in certain urgent situations.
[92] Under s 29 of the Offences against the State Act, 1939, a member of An Garda Síochána, not below the rank of superintendent can issue search warrants under certain conditions in relation to the commission of offences under this Act or treason.
[93] 23 Seanad Deb. (30 June 2009) 433. Senator Ivana Bacik suggested a time period of 24 hours as being more appropriate in situations of urgency.
[94] 1998-II; 27 EHRR 91.
[95] ibid para 30.
[96] ibid para 31.
[97] ibid para 71.
[98] ibid para 73.
[99] *Kopp* (n 94) para 74.

The case of *Valenzuela Contreras v Spain*,[100] (hereinafter *Valenzuela*), also focused on among other areas the lack of judicial supervision. In this case, the applicant's phone was tapped by police who were investigating threatening phone calls being made from an office phone to a female. The police had established that the calls were coming from an office to which the applicant had access. The applicant sought a declaration that his rights under article 8 had been breached on the basis that the statutory basis in Spanish law for the measure taken was not 'sufficiently foreseeable and clear' and that the law was based on the Spanish Constitution which was not clear on the powers available to the Spanish authorities.[101] The applicant also sought relief on the grounds that there was a lack of judicial supervision of the surveillance system. The court, while recognising that the Spanish authorities had in a general sense sought to ensure that the applicant was afforded the maximum protection under the law in operation at the time, nevertheless was still of the opinion that these protections were not clear from a reading of this legislation.[102] The issue of the foreseeability of the law was again a key reason for the court's decision to find that there had been a violation of article 8, with the lack of clarity in both written and unwritten law being a key component of this lack of foreseeability. All these cases make it clear that the ECtHR will strike down legislation that does not have the necessary judicial supervision. It is therefore clear that the three-day approval of a superior officer which in essence gives judicial powers to the issuing officer may breach the court's direction in this area.

The issue of judicial supervision also arises under section 8 of the 2009 Act.[103] This section exempts tracking devices[104] from the definition of a surveillance device. This means that such devices are not the subject of the judicial authorisation. The legislation allows the use of a tracking device for periods of up to four months.[105] Tracking devices provide location data about the objects they are attached to and Gardaí have successfully attached these devices to cars in order to monitor the location of vehicles during covert surveillance operations.[106] However, the devices also provide information on the movement of individuals in vehicles and as such would seem to come under the definition of surveillance under section 1 the 2009 Act. It is not clear why the authorisation for the use of tracking devices could not follow the same procedure for the granting of approval for surveillance warrants under section 7 whereby a superior officer can grant approval in emergencies, which would then be subject to judicial authorisation after a certain period. The argument by the government in excluding tracking devices is twofold. Firstly, it is argued that the devices do not record conversations and as such are less intrusive than other surveillance methods.[107] Secondly, it is argued that the devices often need to be attached in cases of extreme urgency

---

[100] (1999) 28 EHRR 483.
[101] ibid para 43.
[102] ibid para 57.
[103] Under s 8 (1) of the 2009 Act, a member of An Garda Síochána may, for a period of not more than four months or such shorter periods as the Minister may prescribe by regulations, monitor the movements of persons, vehicles or things using a tracking device if that use has been approved by a superior officer in accordance with this section.
[104] Under s 1 of the 2009 Act, a tracking device means a surveillance device that is used for the purpose of providing information regarding the location of a person, vehicle, or thing.
[105] s 8 (1) of the 2009 Act (n 103).
[106] J. Mooney and M. O'Toole *Black Operations: The Secret War Against the Real IRA* (Meath Maverick House Publishers 2003) 62-63. During operations against the Real IRA in the late nineties, the Garda NSU (National Surveillance Unit) was able to take possession of cars that had been stolen by an informant on behalf of the Real IRA. The NSU then attached tracking devices to these cars before the informant then passed the cars onto the Real IRA. As a result, the Gardaí were able to track and intercept bombs, which had been placed in these cars.
[107] 23 Seanad Debates (2 July 2009) 684. See comments of Minister of State at the Department of Justice, Equality, and Law Reform, Deputy John Curran.

and that a court application for warrants may cause undue delay.[108] It is clear that the main aim of the legislation is to focus on the covert recording of the activities of suspects and use this material in criminal trials. In excluding tracking devices from the definition of a surveillance device, the 2009 Act may run into difficulty, as tracking devices clearly appear to constitute an interference with the right to respect to private life under article 8. The ECtHR is very clear on the need for judicial supervision when the State is undertaking such intrusive measures such as covert surveillance.[109] Ashworth questions whether procedures for authorisation by middle ranking officers will satisfy the ECtHR.[110] The grounds that the government have put forward for the lack of judicial control of tracking devices does not seem to reflect the clearly-stated requirement the ECtHR has for such judicial supervision.[111]

4 Is the 2009 Act Adequately Policed?

Section 12 of the 2009 Act makes provision for a High Court judge to review the operation of the surveillance with particular reference to sections 4 to 8.[112] This provision is similar to section 8 of the 1993 Act. The function of the designated judge is extremely important in ensuring that any surveillance undertaken complies with the legislation. The nature of covert surveillance is such that those who are subjected to such surveillance will often not be aware of it. This puts a particular onus on the designated Judge to ensure that these people are protected. In cases where such surveillance does not comply with the law, it is the designated judge who can bring this to light and take the matter further.[113] The ECtHR in *Klass* requires that surveillance laws must have adequate measures against abuse.[114] In the United Kingdom the Communications Commissioner, who oversees the interception of communication in that jurisdiction, produces a detailed report, which is presented to the House of Commons annually.[115] This comprehensive document gives specific details such as the number of authorisations approved,[116] the offences for which the authorisations were approved,[117] and the category of places where communications were intercepted.[118] The report also gives details on problems that have arisen such as poor auditing by senior management and a

---

[108] See also Select Committee on Justice at Committee Stage ETC (11 June 2009) 15. The Minister for Justice, Equality and Law Reform, Dermot Ahern made a similar argument to Deputy Curran for excluding tracking devices from the legislation. His main arguments were that these devices were less intrusive and often have to be attached at short notice and that a Court application might lead to 'a delay that might hinder or jeopardise an investigation.'

[109] *Klass* v *Germany* (n 6).

[110] A Ashworth & M Redmayne 'Gathering Evidence: Reliability, Privacy and Bodily Integrity' in *The Criminal Process* (Oxford Oxford University Press 2005) 114.

[111] D.Walsh *Human Rights and Policing in Ireland* (Dublin Clarus Press 2009) 175. Professor Walsh notes that ideally there will be a judicial element in the *sanctioning* and supervision of surveillance.

[112] s 12 (3) of the 2009 Act states that the functions of the designated judge are to (a) keep under review the operation of ss 4 - 8, and (b) report to the Taoiseach from time to time and at least once every 12 months concerning any matters relating to the operation of those sections that the designated judge considers should be reported.

[113] Under s 12(8) of the 2009 Act where a designated Judge investigates a case under ss (4) and is of the opinion that it is in the interests of justice to do so, he or she may refer that case to the Referee for an investigation under s 11(11).

[114] *Klass v Germany* (n 6).

[115] Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2008-2009 (London: The Stationary Office, 2009).

[116] ibid. See app A, 21.

[117] ibid. See app B, 22.

[118] ibid. See app C, 23 which show whether the places were private homes, a business premises or other location.

failure by those conducting covert surveillance to base their activity on what was authorised as opposed to what was requested.[119] Similarly, the report of the Interception of Communications Commissioner for 2008 gives a detailed account of all intercepted communications carried out by the various authorised bodies in the United Kingdom.[120] The degree of interaction between the Commissioner and those involved in the surveillance is ongoing and in-depth. For example, the Commissioner visits officers undertaking interception work and goes through a sample of warrants to ensure they meet the required standard.[121] The Commissioner discusses various files with the officers concerned to ensure that codes of practice have been followed.[122]

Mr Justice Iarfhlaith O'Neill is the current designated High Court judge assigned to oversee the operation of phone tapping under the 1993 Act and data retention under Criminal Justice (Terrorist Offences) Act, 2005. His most recent report dated 5 December 2008 is a one-page document.[123] The document reports that Judge O'Neill attended at Garda Headquarters, Dublin and later on that day attended at McKee Barracks, Dublin and at the offices of the Department of Justice, Equality, and Law Reform in Dublin on 4 December 2008. Justice O'Neill states that he examined documents and records relating to the operation of the above Acts and spoke with the persons with responsibility for the operation of these Acts at each location. He concludes by declaring that he was satisfied that there was compliance with the provision of the relevant Acts. This report lacks the detail of the similar United Kingdom reports. Information relating to the number of intercepts authorised, internal controls, storage, and security of the intercepted material are not addressed. The case law of the ECtHR has clearly stated there should be sufficient guarantees against the risk of abuse.[124] It is far from certain that a visit once a year by the designated judge followed by a one-page report on all surveillance undertaken in this jurisdiction will meet these guarantees in light of the detailed material that is made available in other jurisdictions.

5 Surveillance and the Garda Síochána Ombudsman Commission

Section 17 of the 2009 Act amends section 98(5) of the Garda Síochána Act, 2005.[125] The Garda Síochána Ombudsman Commission (GSOC) is tasked with investigating complaints against members of An Garda Síochána. This includes investigating arrestable offences committed by Gardaí.[126] It also includes the investigation of incidents where Gardaí are involved and which have led to serious injury and death.[127] This amendment excludes the (GSOC) from any of the provisions of 2009 Act. In other words, the GSOC is not legally empowered to carry out surveillance as part of its investigation of complaints relating to An

[119] ibid 13-14. See common causes of error.
[120] See Report of the Interception of Communications Commissioner for 2008. Commissioner Sir Paul Kennedy presented this report to the United Kingdom parliament pursuant to s 58(6) of the Regulation of the Investigatory Powers Act 2000.
[121] ibid 2.
[122] ibid.
[123] See Report of the Designated Judge pursuant to s 8(2) of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 and the Criminal Justice (Terrorist Offences) Act 2005.
[124] *Liberty, Klass, Valenzuela and Kopp* discussed above.
[125] s 98(1) of An Garda Síochána Act, 2005 states that a designated officer of the GSOC has all the powers, immunities and privileges conferred and all the duties imposed on any member of the Garda Síochána by or under any enactment or the common law. s 98(5) outlines exceptions to s 98(1) namely the Offences Against the State Act 1939/1998 and the Interception of the Postal Packets and Telecommunications Messages (Regulation) Act, 1993.
[126] s 82(1) and s 98 of An Garda Síochána Act, 2005.
[127] s 91 of An Garda Síochána Act, 2005.

Garda Síochána. The Minster for Justice, Equality, and Law Reform justified excluding the GSOC from the provisions of the Act on a number of grounds. Firstly, on the basis that the GSOC was a new organisation and that they needed some time to establish themselves before it was considered prudent to consider giving them the surveillance powers contained in the Act.[128] Secondly, he made the point that the powers contained in the 2009 Act were focused on targeting serious crime and terrorism[129] and that these offences would not be the usual focus of GSOC investigations.

There are a number of potential problems in excluding the GSOC from the 2009 Act. The first issue concerns the ability of the GSOC to investigate complaints against Gardaí when it does not have the same powers. In situations where the GSOC has to investigate serious crime, it will not have the power to carry out surveillance as defined in the 2009 Act. The ECtHR has clearly stated that where it is alleged that State authorities have committed offences, the appropriate investigating authorities should have the same powers to carry out investigations as the agencies of the State have in investigating offences committed by members of the public.[130] In the United Kingdom, the police investigations body namely the Independent Police Complaints Commission (IPCC) has the power to issue authorisations to carry out surveillance.[131] It would have seemed prudent for the legislation to contain some provision whereby the GSOC could request the Gardaí to carry out surveillance on their behalf and under the direction of a senior member of the GSOC. It is clear that the GSOC would not have the surveillance resources available to them in comparison to the Gardaí. This measure would ensure that the legislation would be compatible with the jurisprudence of the ECtHR in this matter and in line with best practices in other States.

E CONCLUSION

From an Irish reader's viewpoint, the decision of the court in *Liberty*[132] is important. In this era of innovative technology, the ECtHR drew a line in the sand at mass surveillance and was not prepared to accept terms such as State security as a legal basis for the monitoring of large amounts of communications traffic. The decisions of the ECtHR have set out in a clear and logical manner the requirements that authorities undertaking surveillance must adhere to. The 2009 Act is a genuine attempt to bring Irish law in this area into line with other countries in Europe. This paper sought to track the evolution of the law in this area focusing on the ECtHR and 2009 Act. Prior to the 2009 Act being enacted there was a clear legislative vacuum in relation to covert surveillance. However, it cannot be stated with any degree of certainty that the 2009 Act in its entirety will pass the legal hurdles that both the Higher Courts in Ireland and the ECtHR will present in light of the potential problems identified in this paper.

---

[128] 30 Dáil Debates (11 June 2009) 26.
[129] ibid.
[130] *Jordan v United Kingdom* Judgment of 4 May 2001, Application no.24746/94 para 107.
[131] Under s 4 of the Independent Police Complaints Commission (Investigatory Powers) Order 2004, senior office holders of the IPCC can issue surveillance authorisations.
[132] *Liberty and Others v The United Kingdom* (n 74).