The Privacy Protection in Electronic Surveillance: a Comparative Research Project between Irish and German Criminal Justice*

*Denis Kennedy / Yukun Zong**

A. Introduction

The tension between the duty of the state to effectively detect and prevent crime from occurring on the one hand, and the right to privacy for private citizens on the other, is an area of the law which possesses many different debate points.[1] Nowadays electronic surveillance has become a measure allowing the state to encroach onto the privacy of individuals very intensively. On this issue the continental European law and the Anglo-American law have different perspectives. Therefore, this piece chooses the German and Irish legal systems to discuss the privacy protection in electronic surveillance in a comparative context. This discussion paper will be divided into two parts, with the first analysing the role that electronic surveillance plays within the Irish jurisdiction by highlighting how Irish domestic law requires further refinement with lessons from German legal instruments and the ECtHR jurisprudence being most pertinent in the protection of human rights. Part two analyses the situation that pertains in the Federal Republic of Germany more closely. More specifically, part one will focus on the implementation of and potential privacy concerns within the Criminal Justice (Surveillance) Act 2009 (hereinafter the '2009 Act'). Part one will also provide evidence of and argue for the immediate amending of the 2009 Act on the grounds that as currently configured, the 2009 Act is in breach of the European Convention on Human Rights (hereinafter 'the ECHR') as determined by numerous decisions delivered by the European Court on Human Rights (hereinafter 'the ECtHR), as well as concerns over its constitutionality within domestic Irish law. Ultimately the paper provides details of how greater specification in privacy infringement can aid both the private citizen and the police authorities in fulfilling their duties correctly. Thus, the paper begins with an analysis of the 2009 Act's remit and its human rights failings.

B. The Irish Response

I. The 2009 Act's scope outlined

Most laws ought to have a purpose and most laws are offered as a response to a potential ill which faces society. The 'ill' that faced Irish society in the noughties was organised crime and feuding criminal gangs in the cities of Limerick and Dublin. In response a cogent effort was made by the Fianna Fáil/Green Party government coalition to tackle the advancement of the criminal threat to Irish society. The 2009 Act is an example of this response. The 2009 Act's intention was to enable evidence which was garnered by covert surveillance to be used in a criminal trial where previous to July 2009 such evidence would not have been deemed admissible in a court of law.[2] The intention was to allow the admissibility of evidence to be more easily admitted as it would, for the first time in Irish criminal law, allow mainly the Gardaí, but not limited to that force, to avail of the increased advantages of electronic surveillance to curb criminal activity.[3] New legislation was warranted and it arrived with the 2009 Act defining surveillance in section 1 as:

> *... (a) 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."*[4]

The Garda's superior officer does not have to identify an arrestable offence specifically, however this superior officer must be, at the time an application is made for authorisation to commence surveillance, investigating an arrestable offence.[5] These are the issues which affect the 2009 Act's scope; however its application is of most concern from a privacy perspective.

II. The Independent Judicial Scrutiny Issue

The application of the 2009 Act is felt most prominently when the issue of how an authorisation is granted to a Garda is considered. First, in situations which are 'urgent', a Garda member can apply for an 'approval' from a superior officer

* This article was presented on the 8th Annual Graduate Conference of the Centre for Criminal Justice and Human Rights (CCJHR) at University College Cork on on the 5th and 6th June, 2014. Denis Kennedy, LL.B., LL.M. B.L., is Ph.D. candidate at the 'Centre for Criminal Justice', University of Limerick since 2014, specialising in research concerning the exclusionary rules of evidence in criminal trials and criminal theory. Yukun Zong, LL.M., is Ph.D. candidate at the Max Planck Institute for Foreign and International Criminal Law in Freiburg i. Br. since 2010, researching on the theme: Exclusionary rules in criminal procedure, a comparative research project in German, U.S. and Chinese law. She has studied law at Hebei University of Economics and Business from 1999 to 2003 and China University of Political Science and Law from 2004 to 2007.

1 Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 (5) The Harvard Law Review 193-220.

2 Anne-Marie Whelan, 'Are They Watching You?- The Criminal Justice (Surveillance) Act 2009' (2010) 1 The Bar Review 2-5, 2.

3 The main reason as to why prior to 2009 such covert surveillance which was in common practice amongst Garda members could not be admissible was the lack of a statutory framework with which to work for the members in question. The Act applies to the Garda Síochána in respect of arrestable offences (those offences for which there is a five year or more prison term applicable), to the Defence Forces where the 'security of the State' is at issue and the Revenue Commissioners with regard to a list of revenue offences as detailed under section 4 of the 2009 Act.

4 Criminal Justice (Surveillance) Act 2009, s. 1.

5 A 'superior officer' is defined within the 2009 Act as an officer 'not below the rank of Superintendent'.

who is also within the same unit which will conduct the surveillance operation.[6] The worrying aspect arrives from the fact that independent judicial scrutiny which, appears to be the bedrock of the 'authorisation' procedure, will be by-passed entirely when a case is deemed 'urgent'. Admittedly, the time limit of seventy-two hours for an approval to be held valid is a factor which may allay some fears, but not completely. It is the process by which a case is deemed 'urgent' and by whom it is deemed to be so that is the cause for most concern. It is submitted that the present mechanism effectively eliminates one of the most important safe-guards for a private citizen who would expect that an independent voice would have been heard before such a grave interference with their constitutional and privacy rights was permitted. Note also the alteration in language, where an 'authorisation' becomes an 'approval' which, it may be argued is but a mere point of legislative semantics, however such subterfuge is unwelcome. The 'authorisation' can last for up to three months from the date upon which it was issued.[7] This period can be renewed and how many times it can be renewed is not made absolutely clear under the 2009 Act's provisions.[8]

III. The 'Approval' v 'Authorisation' Criteria

Under section 5 of the 2009 Act a District Court judge of any district area within the jurisdiction can issue an authorisation in an *ex-parte* hearing.[9] Under section 7(3) of the 2009 Act, more specific criteria are delineated as to when a partial 'approval' may be granted by a Garda superior officer, such as if the suspect is at risk of absconding, if there is a risk that evidence (regardless of how trivial it might be) may be destroyed or if the 'security of the State' is at risk.[10] It is conceded that senior Garda officers already possess the statutory power to issue search warrants under certain defined scenarios.[11] The single most pertinent cause of concern however is the fact that Gardaí can avail of a wide range of potential offences with which to attach an approval, as long as it falls within the definition of an arrestable offence. This is arguably far too expansive for covert surveillance to be approved without some semblance of independent judicial oversight. Such a lack of independent oversight is compounded by the fact that the approval lasts for seventy-two hours which in itself is a debatable period of time without judicial intervention.[12] As Barry suggests, each District Court area should have a District Court judge 'on-call' in order to make the infringement upon human rights the least oppressive without judicial scrutiny of the matter.[13] The District justice is already 'on-call' in each District Court area to accommodate emergency special sittings over week-ends or holiday periods, which means that an alternative is already available.

IV. The Idah v Director of Public Prosecutions judgment

The Court of Criminal Appeal (hereinafter 'the CCA') in Dublin delivered a judgment in January 2014 in a case which directly concerned the provisions of the 2009 Act.[14] It is a relevant case in that the court's judgment sets out how an investigation, which incorporates covert electronic surveillance, can retain the proportionality requirement, which is essential in any infringement upon a constitutional right in Ireland. Furthermore, the case involves the categorisation of which surveillance method ought to be utilised in certain circumstances. The appellant argued that the recordings admitted into evidence at his trial were compiled outside the provisions of the 2009 Act and therefore should not have been admitted into evidence. The Gardaí had been authorised by a District Justice to plant a surveillance device in a room in a prominent hotel in Dublin between the 14th-18th September 2010 inclusive, however no meetings took place in this room and the recordings resulted from a different surveillance device which had not been authorised, which the Gardaí had planted elsewhere in the hotel's environs.

It transpired that a superior officer within the Garda Síochána had issued an approval on the 19th September 2010 for further surveillance to be conducted on this day only. Notably, no attempt had been made by the Gardaí to seek judicial authorisation for any further surveillance on the 17th, 18th or 19th of September when the Gardaí could have done so. It was held, inter alia, by the panel of the CCA (MacMenamin J, with Herbert and de Valera JJ. concurring) that the recordings made during the period 14th-18th September 2010 were admissible because the trial judge retains a deciding discretion with regard to evidence admissibility under section 14(4) of the 2009 Act. However, in relation to the evidence obtained on the 19th, the CCA held that this was illegally obtained, resulting in the quashing of the appellant's conviction and a re-trial being ordered. MacMenamin J, delivering the judgment of the CCA, held in particular that in order for an 'approval' to be issued validly by a superior Garda officer, one of the urgency requirements which are detailed under section 7(2) of the 2009 Act would have to be satisfied first. Consequently, due to the fact that no evidence was adduced by the prosecution to support which 'urgent' condition was being satisfied which necessitated an internal Garda 'approval' to be issued rather than an

[6] Criminal Justice (Surveillance) Act 2009, s. 7.
[7] Ibid, s. 5(8).
[8] This could effectively result in a person being placed under surveillance for an indefinite period of time, so long as the judicial authorisation is renewed or the circumstances of the case requiring such surveillance changes dramatically.
[9] This could mean that a District judge in Donegal could award an authorisation for surveillance in Cork which would raise further issues as to the level of independent scrutiny that could be delivered by that judge.
[10] Criminal Justice (Surveillance) Act 2009, ss. 7(1) and 7(2).
[11] Criminal Justice (Drug Trafficking) Act 1996, s. 8(1) amends the Misuse of Drugs Act 1997, s. 26; Offences against the State Act 1939, s. 29.
[12] *Seanad Debates* (30th June 2009) 433 where Senator Ivana Bacik suggested that a period of 24 hours would be more appropriate, but this was not followed, these sentiments were also echoed by Fergus O'Dowd, T.D. in the Bill's Second Stage in the Dáil.
[13] John Barry, 'The Criminal Justice (Surveillance) Act 2009: An Examination of the Compatibility of the New Act with Article 8 of European Convention on Human Rights' [2010] Cork Online Law Review 1, 12.
[14] *Idah v D.P.P.* [2014] IECCA 3, CCA No. 164/2012. The facts of the case can be stated briefly as that the appellant was convicted and sentenced of soliciting another to commit the offence of unlawful importation of cocaine from Brazil to Ireland. The appellant had solicited two undercover Garda members to travel to Brazil for importation purposes. Throughout the trial at first instance, audio recordings from a surveillance device, which was installed in a hotel room where the appellant and the Garda members met, were admitted into evidence.

'authorisation', the evidence gathered on the 19th was illegal and inadmissible.

V. Significance of the Idah Judgment

Throughout the course of his judgment, MacMenamin J cited the right to privacy within the context of the 2009 Act's application. He paid particular care to mention that this right is not absolute and can, in certain circumstances, be curtailed in accordance with the law. The learned judge also cited *Ludi v Switzerland* in which the ECtHR held that when one is involved in a criminal enterprise, their expectation of privacy protection is inherently less than that of a person who was not involved in criminal activity.[15] It appears then that the issue as to whether proportionality is adequately protected falls on the decision to either obtain an approval (internal mechanism) or an authorisation (external mechanism). In this regard in *D.P.P. v Peter Byrne* Hardiman J, in the Supreme Court, was faced with interpreting section 8(2) of the Criminal Justice (Drug Trafficking) Act 2006 (hereinafter 'the 2006 Act').[16] Hardiman J stated:

> *They [the Gardaí] must apply to a judge or a peace commissioner unless the very limited circumstances which permit them to apply to a superintendent are present. These [urgent] circumstances must be demonstrated to be present for the superintendent's warrant to be valid.*
>
> [*Brackets added by authors.*]

Clearly, the superior courts in Ireland will seek a clear demonstration that one of the urgency criteria has been satisfied which sets the parameters of the proportionality of any intended infringement on the rights of the suspect, however the provisions of s. 14 (4) of the 2009 Act allows for a very wide ambit of which surveillance techniques may be used, which arguably places any suspect in an invidious position regarding their right to privacy, which has been subject to constitutional protection in Ireland.

VI. Is the 2009 Act fit for purpose?

Even if the independent judicial oversight is stated clearly by the 2009 Act for surveillance periods which are longer than seventy-two hours and are not within the 'urgent' category, it is also quite obvious that an infringement on a citizen's right to privacy is impacted upon. Most *ex-parte* applications, which is what an 'authorisation' application will be, are dictated to a large extent by the evidence which is proffered by the applying Garda members who will offer such evidence that will be difficult for a District Justice to contradict. This will often mean that due to the limitations of the *ex-parte* process, the District Justice will have to adjudicate on the merits of the application with just one side of the evidence being made available in the application. When one considers that the 2009 Act's powers involve a serious infringement on the right to privacy, the question remains as to whether this biased process is fit for purpose? This is all the more cogent when one remembers that the surveillance may record people and conversations which have nothing to do with any potential Garda investigation into an arrestable offence. Furthermore, even if evidence is obtained whilst the terms of the 2009 Act are flouted, such evidence is not automatically deemed inadmissible.[17] Additionally, the 2009 Act's review by a serving High Court judge is not going to be able to provide any real assistance in the correct regulation of the infringement onto privacy, as such a review is meant to be only a snap-shot of how the 2009 Act has operated in that review year.

Therefore, a suspect who is subject to the 2009 Act's provisions must be able to find out under which circumstances the Irish provisions will be activated. This is a fundamental tenet of the theory of the rule of law. For instance, in *Weber & Savaria v Germany* the ECtHR held that:

> *The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures.*[18]

This is not the case in the Irish law as too much authority is placed within the hands of the Gardaí in particular, along with the other personnel who can avail of the 2009 Act's provisions. For instance, under section 8 the use of a 'tracking device', which can reveal much personal information, does not have to succumb to independent judicial assessment to be activated on a suspect's vehicle. Furthermore, under section 8 (3) a tracking device is allowed to be inserted with the issuing officer being effectively placed in the position of a District Court judge in deciding that had the matter gone to an *ex-parte* hearing, it would have been authorised anyway. This is effectively replacing the role of a judge with that of a police officer in judging the necessary infringement upon a person's constitutional right to privacy.

VII. The constitutional protection of privacy in Ireland

The Constitution of Ireland protects the fundamental rights of citizens in the enjoyment of privacy under Article 40.3.[19] Specifically, in *Kane v Governor of Mountjoy Prison* the Supreme Court held that a person has the right to the enjoyment of privacy and that unwarranted surveillance could, in certain circumstances, be an infringement of that person's constitutional right to privacy.[20] Note too that Article 40.5 of the Constitution describes and protects the sanctity of the dwelling by providing that the dwelling place "…shall not be forcibly entered save in accordance with law."[21] The central test under the Irish Consti-

[15] [1992] 50 E.H.R.R. 173.

[16] [2003] 4 I.R. 423; section 8 (2) of the 2006 Act allows a senior Garda officer to internally issue a search warrant in times of urgency similar to those specified within the 2009 Act.

[17] Whelan, 'Are They Watching You?' (2010) The Bar Review 2, 4.

[18] *Weber & Savaria v Germany* (ECtHR, App No. 54934/00), para. 93.

[19] Constitution of Ireland 1937, Article 40.3.1 and 2 states: The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen. 2° The State shall, in particular, by its laws protect as best it may from unjust attack and, in the case of injustice done, vindicate the life, person, good name, and property rights of every citizen.

[20] [1988] 1 I.R. 757.

[21] Constitution of Ireland 1937, Article 40.5.

tution is whether the interference to a person's right is in accordance with a 'legitimate aim' and whether the interference is 'proportionate'.[22] What is meant by 'proportionate' has been elaborated upon by the Irish superior courts in *Heaney v Ireland*.[23] Costello J laid down the criteria for a 'proportional' infringement of a constitutional right when stating:

The means chosen must pass a proportionality test. They must:

> *(a) be rationally connected to the objective and not be arbitrary…*
>
> *(b) impair the right as little as possible; and*
>
> *(c) be such that their effect on rights are proportional to the objective.*[24]

With this quite detailed explanation offered by Costello J it is at least arguable that the provisions of the 2009 Act, in relation to the 'approval' mechanism, are in contradiction to the outlined three-pronged proportionality test in Ireland. Furthermore, in *Kelly v Dublin City Council and the Attorney General* the High Court held that if a fundamental right was to be curtailed, the decision to infringe upon such a right must be proportionate.[25] Crucially, however, Peart J held that in order to evaluate the proportionality requirement, the affected party must be given an opportunity to be heard before any infringement could take place. This case offers a clear indication that the High Court will seek clarification that the other side has been properly heard when the proportionality requirement, which is a prerequisite element, is to be assigned to any action which will impact those rights. It is therefore submitted, that this requirement cannot be met by the provisions of the 2009 Act as currently constituted as the person whose rights are being impacted upon cannot, and will not, be heard by an independent tribunal. The constitutionality of the 2009 Act is at least doubtful in this regard, particularly when analysed further through the spectrum of European jurisprudence.

VIII. The ECtHR's treatment of privacy

The European Court on Human Rights in Strasbourg (hereinafter 'the ECtHR') has ruled on the issue of privacy and the impact of surveillance upon that right. It is not possible here to provide a complete review of the ECtHR's jurisprudence on the matter; however a brief analysis will suffice for present purposes. Thus, in *P.G. and J.H. v United Kingdom* the ECtHR held that what was an important factor in determining whether the right to privacy under Article 8 of the European Convention on Human Rights (hereinafter 'the ECHR') was infringed is the 'reasonable expectation' that a person would have of privacy.[26] In *P.G. and J.H.* the ECtHR held that there was an infringement on Article 8 as both applicants' voices had been recorded and analysed all in a police station.[27] In *Malone v United Kingdom* the ECtHR stated that there must be:

> *…a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by [Article 8.1]*.[28]

Similarly, in *Klass v Germany* the ECtHR held that:

> *…the Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse*.[29]

Interestingly, the ECtHR in *Klass* held that there was no breach of Article 8 due to the fact that there were strict process criteria set down within the domestic German legislation, which also stipulated under which conditions the use of covert surveillance could be used. It is arguable therefore, whether the 2009 Act would meet with such acquiescence by the Strasbourg court.

VIIII. Can Ireland learn from the United Kingdom?

If Ireland could possibly gain assistance from our immediately neighbouring jurisdiction, which shares the traditions of the common law in relation to covert surveillance and its application, necessary amendments to the 2009 Act may be made more efficiently. The Regulation Powers Act 2000 (hereinafter 'RIPA') came into force in the United Kingdom on the same day as the Human Rights Act 2000 was passed by parliament. Section 27 of RIPA defines what is meant as 'intrusive surveillance' as being:

> *…covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device*.[30]

Any surveillance which fits within the definition of section 27 can only be authorised by the Home Secretary, a Chief Constable, the Director of the Serious Organised Crime Agency, a designated official within Her Majesty's Revenue and Customs, and the chairman of the Office of Fair Trading. If the authorisation is issued by one of the above office holders, it must be made with the belief that it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime or if it is in the economic well-being of the country to do so. The same proportionality element is also inserted as a factor to which the issuer of the authorisation must recognise. From this remove it is questionable if the

[22] *King v Attorney General* [1981] I.R. 233, 257.
[23] [1994] 3 I.R. 593.
[24] Ibid, 607.
[25] [2012] IEHC 94; High Court, Peart J.
[26] ECtHR Unreported, 25 September 2001, Application No. 44787/98, para. 57.
[27] The European Convention on Human Rights, Article 8 (2) states: '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 wellbeing 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.'
[28] ECtHR, Unreported, 2 August 1984. Article 8.1 states: 'Everyone has the right to respect for his private and family life, his home and his correspondence.'
[29] ECtHR, 6 September 1976.
[30] The Regulation Powers Act 2000 (UK), s. 27.

terms of the RIPA legislation could aid the Irish legislator in improving the 2009 Act so that human rights are better protected. Moreover, the RIPA provisions do not enhance the independent scrutiny element which is required to any greater extent than what is currently present in Ireland.

X. Part one conclusion

In concluding this part, the Irish law in relation to covert surveillance lacks both certainty and transparency in the protection of a fundamental right such as privacy. It is to be hoped that when one looks to other jurisdictions for guidance as to how Irish law in this area may be improved, Irish legislators will possess the motivation to learn from similar experiences in those jurisdictions. Thus, part two outlines in what ways the issue of covert surveillance are dealt with in Germany, with reference to both German constitutional and legal principles.

B. German Electronic Surveillance

I. The basics of German surveillance regulation

By way of context, in Germany there are four kinds of electronic surveillance. First, there is the telecommunication surveillance (§§ 100 a, 100 b StPO). This kind of surveillance includes telephone, mobile telephony, telefax, e-mail and internet telephony surveillances. The second type is the acoustic surveillance inside a room (§§ 100 c, 100 d StPO). This kind of surveillance is limited to just acoustic surveillance, i.e. the spoken words in a room. The third example is the acoustic surveillance outside a room (§ 100 f StPO), this kind of surveillance means the same as the second type, but outside the room. The last type is the observation outside a room (§ 100 h StPO), i.e. photographing, filming, video, making satellite photos, beeper devices, night vision devices, direction finding and GPS all come under this surveillance strand. The last four means (i.e. beeper devices, night vision devices, direction finding and GPS) of surveillance do not include spoken words (this comes under § 100 f StPO) and pictures (this is already included in the first means with regard to photographing under § 100 h StPO). But for a video surveillance for a longer period of time, for example a non-stop video surveillance for more than twenty-four hours or a video surveillance for more than two days, not only is § 100 h sec. 1 s. 1 (2) StPO applied, but also § 163 f StPO. A total surveillance or an 'all-over' monitoring process that can record the suspect's profile will be against the principle of proportionality and not allowable as evidence.[31]

The German electronic surveillance system has different intensive degrees of intrusion onto privacy. The most intensive is the second type as outlined, the acoustic surveillance of a room. After that comes the telecommunication surveillance. Except the last mode of surveillance, which is the observation outside a room,[32] (the mildest intrusion onto privacy), all the other surveillance methods can be used only if a serious crime is under investigation. Generally the regular investigating methods would not be adequate in order to investigate these crimes or other investigating methods have disproportional difficulties. These crimes cover not only organised crime but also crimes concerning the security of the State, terrorism, murder and robbery. Only if there is a listed serious crime under investigation may the constitutional rights of the suspect take precedence over the public interest which lies in the thorough investigation of the offence by the police authorities.[33]

In Germany, the police investigation comes under the guidance of the prosecutor. Generally, the prosecutor makes the application for an electronic surveillance at a court which is approved if the application meets the requirements of the surveillance mode that is to be used. This is the "Richtervorbehalt" principle which means that only the judge is responsible for issuing the warrant to undertake certain investigating measures in Germany. During the approval process, each party to the case is not heard because at this time it is not yet a full criminal trial. Permission for both the telecommunication surveillance and the acoustic surveillance outside a room can be issued by a court or the prosecution department if it is needed 'urgently'. But the decision to undertake these surveillances from the prosecution department must be approved by a court within three working days. [34] For the acoustic surveillance inside a room however, it should be ordered only by a court or the president of the court if it is required urgently. The president's decision must be approved by the court again within three working days.[35] The last kind of surveillance, which is the observation outside the room, can be ordered by either the prosecution department or the police.[36] Principally an electronic surveillance is executed against the defendant and under certain requirements against other persons. Some suspects with occupational or similar exemptions cannot be monitored under specified circumstances.[37] The acoustic surveillance in a room should not be more than one month.[38] The other kinds of surveillance, except the observation outside the room, cannot be undertaken for more than three months.[39] However, it is also permissible for a surveillance order to be extended so long as the requirements for ordering such surveillance necessitate taking account of the investigation's results.[40]

II. Privacy protection in the electronic surveillance

The protection of privacy is displayed in the law of electronic surveillance in Germany in several ways. Firstly, the privacy protection is demonstrated in the requirements for an order for an electronic surveillance to be granted by the court. All kinds of surveillance can be used for the investigation of serious crimes, but only if regular investigating measures could not adequately assist the police in their work. Herein lies the "proportionality" in the requirements for an order to be issued by the court. In other words, if there are some other measures which can achieve the investigation goal, the electronic surveillance should not be undertaken. The judicial examination,

[31] Amin Nack, Karlsruher Kommentar zur StPO, 6th Ed. § 100 h, marginal no. 5.
[32] § 100 h StPO.
[33] Decision by BayObLG, Juristische Rundschau [1983], 124, S. 125.
[34] § 100 b sec. 1 and § 100 f sec. 4 StPO.
[35] § 100 d sec. 1 StPO.
[36] Lutz Meyer-Goßner/Bertram Schmitt , Kommentar zur StPO, 54th Ed. § 100 h, marginal no. 10.
[37] § 160 a sec. 1, § 148, § 100 c sec. 6 s. 1 and 2 StPO.
[38] § 100 d sec. 1 StPO.
[39] § 100 b sec. 1 and § 100 f sec. 4 StPO.
[40] § 100 b sec. 1, § 100 d sec. 1 and § 100 f sec. 4 StPO.

pertaining to allowing surveillance to operate, can also give a guarantee for the protection of privacy. Additionally, there is a limitation on the those who can be monitored. The electronic surveillance should observe these requirements to limit the intrusion onto the privacy of concerned persons.

Secondly, the 'corn sphere' of the private life of concerned persons must not be infringed through electronic surveillance. In Germany, there is a theoretical basis which has been established by the German constitutional court in Karlsruhe. This theory is called 'the sphere theory' or 'the three rungs theory'.[41]

The first sphere (or rung) is the 'corn sphere' of the private life. This is the intimate and untouchable sphere of human freedom, where the public intrusion cannot be allowed. This 'untouchable sphere' is grounded in law in Article 1 section 1 and Article 2 section 1 of the German Constitution.[42] The surveillance in this area is strictly prohibited. The private interests here are dominant in comparison to the interests of investigating a possible crime.[43] The German constitutional court has stated that several elements must be considered in deciding whether an area belongs to the 'corn sphere' of private life. Consideration must be given as to whether the concerned person keeps personal information secret, whether the contents have a highly personal character and how this information may affect the area or interests of others and the society in general.[44] If it concerns the hatching of a plan for a crime or a committed crime, the content is then not in the 'corn sphere' of private life.[45] The German criminal procedure code states in § 100 c that two elements are to be considered: one is the place where the conversation is taking place; the other is who is actually speaking. Usually conversations with very personal, confidential people,[46] for example with close family members,[47] a psychotherapist or clergy,[48] criminal attorney, physician under certain circumstances[49] and with close friends in some situations,[50] are to be considered as being within the 'corn sphere' of private life. Conversations in common work areas do not belong in the 'corn sphere'.[51]

This "corn sphere" of private life can be touched during telecommunication surveillance, acoustic surveillance in a room and outside the room, but it must be decided on the facts of the case. For the first two surveillances, the German code of criminal procedure[52] has clearly stated that if there are actual indications that the surveillance could touch the 'corn sphere' of private life, the application for this surveillance should not be approved. If, during the acoustic surveillance inside a room, the personal information which is considered to come within the 'corn sphere' is overheard, then the surveillance must be stopped.[53]

However, the provisions concerning the corn sphere of private life are not without problems. The regulation § 100 a sec. 4 s. 1 StPO states that the application should not be approved if there are substantive indicators showing that the surveillance gathered would only be information that is within the parameters of the corn sphere. This regulation's application has been criticised by academics,[54] who say that it has a mere symbolic meaning.[55] That is because in practice, many conversations concerning both highly personal information and other information that is not highly personal. Another criticism is that the other parts of the conversation could not be understood if the highly personal part is extracted because the conversation loses its meaning.[56]

The second rung is the private sphere. In this sphere the citizen, as a person of the community, must accept some intrusion into his privacy by the state, so long as no intimate sphere is penetrated[57] and the general interest in an effective investigation outweighs the personal interest in keeping the information secret, and if the proportionality principle is safeguarded.[58] An example would be a conversation about a crime in a private room or with a wife and husband on the phone.

The third rung is the social sphere. In this sphere the surveillance can be taken generally. The protection area according to Article 1 section 1 and Article 2 section 1 of the German Constitution would not come under the third rung. But some kinds of surveillance taken in this area can also touch the corn

[41] Decisions from the German constitutional court: BVerfGE 6, 32; BVerfGE 27, 1; BVerfGE 27, 344; BVerfGE 32, 373; BVerfGE 33, 367; BVerfGE 34, 205; BVerfGE 34, 238. Literature: Birgit Laber, Die Verwertbarkeit von Tagebuchaufzeichnungen im Strafverfahren [1995], S. 15 and S. 22-30; Karl Heinz Gössel, Die Beweisverbote im Strafverfahrensrecht der Bundesrepublik Deutschland, Goltdammer's Archiv für Strafrecht [1991], 483, S. 501 ff.; Georg Küpper, Tagebücher, Tonbänder, Telefonate – Zur Lehre von den selbständigen Beweisverwertungsverboten im Strafverfahren -, Juristische Zeitung [1990], 416, S. 418.

[42] Decision form the German constitutional court, BVerfGE 37, S. 1, S. 8.

[43] Decisions from the German constitutional court: BVerfGE 34, 205, S. 245; BVerfG, Neue Juristische Wochenschrift [2007], 2753, S. 2756.

[44] Decision form the German constitutional court: BVerfG, Strafverteidiger [1990], 1, S. 2.

[45] Decision from the German constitutional court: BVerfG, Strafverteidiger [1990], 1, S. 2; Theodor Kleinknecht, Beweisverbote im Strafprozess, Neue Juristische Wochenschrift [1966], 1537, S. 1540.

[46] Ulrich Eisenberg, Beweisrecht der StPO, 7th Ed., marginal no. 2492; decision from German constitutional court: BVerfGE 109, 276, S. 322.

[47] Lutz Meyer-Goßner/Bertram Schmitt, Kommentar zur StPO, 54th Ed. § 100 a, marginal no. 24a; Jürgen Wolter, Systematischer Kommentar zur StPO, § 100 a, marginal no. 55; decision from German constitutional court: BVerfGE 109, 276, S. 317.

[48] Lutz Meyer-Goßner/Bertram Schmitt, Kommentar zur StPO, 54th Ed. § 100 a, marginal no. 24a; decision from the German constitutional court: BVerfGE 109, 276, S. 317.

[49] Lutz Meyer-Goßner/Bertram Schmitt, Kommentar zur StPO, 54th Ed. § 100 a, marginal no. 24a; decision from the German constitutional court: BVerfGE 109, 276, S. 322 and 323.

[50] Jürgen Wolter, Systematischer Kommentar zur StPO, § 100 a, marginal no. 55; Jürgen Wolter, Alternativen zum Regeirungsentwurf 2007 zur Neuregelung der Ermittlungsmaßnahmen, Goltdammer's Archiv für Strafrecht [2007], 183, S. 196; decision from German constitutional court: BVerfGE 109, 276, S. 322.

[51] § 100 c sec. 4 StPO.

[52] § 100 a sec. 4 and § 100 c sec. 4 StPO.

[53] § 100 c sec. 5 StPO.

[54] Ulrich Eisenberg, Beweisrecht der StPO, 7th Ed. marginal no. 2492; Jürgen Wolter, Alternativen zum Regeirungsentwurf 2007 zur Neuregelung der Ermittlungsmaßnahmen, Goltdammer's Archiv für Strafrecht [2007], 183, S. 196-197.

[55] Jürgen Wolter, Systematischer Kommentar zur StPO, § 100 a, marginal no. 57.

[56] Amin Nack, Karlsruher Kommentar zur StPO, 6th Ed. § 100 a, marginal no. 41.

[57] When the corn sphere is touched depends on the situations of the case. See the decision from the German constitutional court, BVerfGE 34, 238, S. 248.

[58] Decisions from the German constitutional court: BVerfGE 34, 238, S. 246; BVerfG, Strafverteidiger [1990], 1, S. 2; Kathrin Janicki, Beweisverbote im deutschen und englischen Strafprozess [2002] S. 147.

sphere of private life, for example the acoustic surveillance outside a room. However, these would be decided upon the facts of the case usually.[59]

Thirdly, the exclusion of evidence also plays a role in the protection of privacy in electronic surveillance law in Germany. If the corn sphere of private life was penetrated during an electronic surveillance, then the overheard information could not be used as evidence at the trial.[60] That is because the private interest in the corn sphere is untouchable and the State authorities must not intrude onto this area. If information from the private sphere, the second rung, was caught the question whether it could be used as evidence depends on the situation of the case.[61] The German courts use a 'weighing of interests' test to decide whether the information can be used. In the process of the weighing of interests there are several elements to be considered, and they include: the severity of the intrusion onto the right to free development of personality,[62] the alleged offence to which the surveillance is being applied, the specific wrongdoing and the overall evidence in an individual case. [63] If the private interest outweighs the public interest in seeing an effective investigation, the information from the surveillance should not be used as evidence in the trial.

Fourthly, every year the federal states and the general federal prosecutor compile reports about the telecommunication surveillance and acoustic surveillance in a room and these reports are published on the internet.[64] This administrative measure can also put the privacy protection in electronic surveillance under control.

III. Cases concerning privacy protection in electronic surveillance

In *LG Ulm, Strafverteidiger* [2006] S. 8, the prosecutor wanted to apply for a telecommunication surveillance against the sister of the defendant who allegedly had committed a bank robbery in Ulm and her accomplice, because according to the intelligence from another telecommunication surveillance, the prosecutor had learnt that the two suspects might be message mediators for the defendant. In respect of the constitutional rights of third persons the court thought these rights must be safeguarded and confidential communications between third persons could not be encroached upon excessively.[65] Only the calls from the defendant to the telephones of these two suspects or the calls that the defendant made from the suspects' telephone could therefore be monitored.[66] The court weighed the interest of an effective investigation in the bank robbery against the protection of constitutional rights of third persons, and it also viewed the fact that there was no correlation between the users of the telephone connections and the alleged crime.[67] Consequently, the surveillance in this case was not proportional and therefore was not admitted as a result.[68]

The second case *BGHSt 31*, S. 296 decided by the highest federal court in Germany is a case concerning a situation between a telecommunication surveillance and an acoustic surveillance in a room, but the court deemed it as a case in telecommunication surveillance. In this case the defendant had not put down the monitored phone correctly so that the conversation between the defendant and his wife in the living room could still be overheard. The court held that the recording of the conversation between the close family members had penetrated the corn sphere of private life, so this surveillance was not usable either.[69]

The last case is *OLG Düsseldorf, Neue Zeitschrift für Strafrecht* [2009] S. 54 which concerns the acoustic surveillance in a room. Based on the statements of the defendant the prosecutor had expected he and his wife would talk about the crime and exchange their statements in their private apartment. The prosecutor had applied for an acoustic surveillance in a room. The *OLG Düsseldorf* court applied the decision of the German constitutional court which held that not every connection between the crime and defendant's statements would be sufficient to indicate that information would fall outside the corn sphere.[70] Otherwise every expected mixed conversation, which includes both criminal and non-criminal evidence, could lead to a monitoring because it cannot remove the possibility that a defendant could talk with his close friends about a crime.[71] The court stressed that there must be substantive indicators showing that the surveillance would not intrude upon the corn sphere of the private life of suspects. But in this case the prosecutor had not provided such indicators, but only an assumption. The prosecutor's application was therefore rejected.

C. Conclusion

In Germany the privacy protection in electronic surveillance covers many aspects. To protect the citizen's privacy there is not only a judicial scrutiny but also very clear regulation about what content should not be overheard. The legislation says that the monitoring must be stopped if during the monitoring process the corn sphere of private life is overheard and such information could not be used as evidence at trial. The protection is seen from the initial application to the trial itself. Judicial

[59] Decision from the German Federal High Court: BGHSt 53, 294, S. 304.
[60] § 100 a sec. 4 and § 100 c sec. 5 StPO.
[61] Decision from German constitutional court: BVerfGE 34, 238, S. 250. Kathrin Janicki, Beweisverbote im deutschen und englischen Strafprozess [2002] S. 147.
[62] The right to "free development of personality" is mentioned in the Article 2, section 1 of the German constitution, which states "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law." This right has two prongs. The first is the right of freedom of action which is very comprehensive. The other is the general personal right deduced from Article 2 section 1 and Article 1 section 1 of the German constitution and it is based on human dignity. The latter protects a sphere of privacy which is absolutely inviolable. This second right is actually what the German Constitutional Court meant in this sentence. In this general personal right a person can develop his personality according to his notion without external control. The general personal right protects the private sphere, self-determination and self-expression. See Christoph Groepl/Kay Windthorst/Christian von Coelln, Studienkommentar zum Grundgesetz [2013] S. 52-80.
[63] Decision from German constitutional court: BVerfGE 34, 238, S. 250.
[64] § 100 b sec. 5 § 100 e StPO.
[65] Decision from the regional court in Ulm: LG Ulm, Strafverteidiger [2006], 8, S. 9.
[66] Ibid.
[67] Ibid.
[68] Ibid.
[69] Decision from German Federal Highest Court: BGHSt 31, 296, S. 299.
[70] Decision from the German constitutional court: BVerfGE 109, 279, S. 319.
[71] Decision from the regional appeal court Düsseldorf: OLG Düsseldorf, Neue Zeitschrift fur Strafrecht [2009], 54, S. 55.

scrutiny would not be enough to guarantee privacy protection. But in Ireland it seems that the protection concentrates on the judicial scrutiny before the undertaking of the surveillance, or at least people there place more weight on such scrutiny in the privacy protection.

There is a corn sphere of private life which cannot be interfered with in Germany. This sphere is one of the three spheres in the German 'sphere theory'. Within this theory an interest's weighting is actually taken to decide whether the private interests weigh more than the public's interest in having the investigation conducted thoroughly. The proportionality-principle is also taken into account in this interest's weighting. In Anglo-American law such interest weighting may be called 'interest balancing'. They actually mean the same in practice. But in Anglo-American law no hierarchy or structure of privacy is developed as seen in Germany. Although in Germany the court has also to decide which interest is greater than the other according to the cases, but there is some guide lines such as sphere theory for a case deciding. Is there such a guide line in Ireland?

Both German and Irish law does not require a hearing of all parties before issuing a surveillance authorisation. There is maybe no significant difference at judicial approval in practice. In Ireland it sounds like a great problem that the two parties are not heard by a judge before they issue an authorisation. In Germany people do not think that this is a grave problem, although there is also a suspicion that the judge can make errors in the decision. Generally Germans trust the judges and think they can make a fair and correct decision about whether the corn sphere could be touched by the surveillance. There is an admissibility scrutiny just to check whether the application meets the requirements of the surveillance. If the electronic surveillance has penetrated the corn sphere or the privacy excessively, there is also an exclusionary rule for the evidence and the information could not be used at trial.

In Anglo-American law it would be thought as being unfair if a decision is not made by a judge on the basis of a hearing of both parties. This is because it is an adversary process, but in Germany the inquisatory model is used. The judge directs the trial and all the parties trust the judge to do so. So there may be a problem if the judge has not heard the parties before deciding to issue an order to monitor in Ireland, but in Germany this would not be the case.

Ultimately, this paper has attempted to give a flavour of the contrasts that are seen between two different legal systems. At the outset, it may surprise some observers to note just how similar both systems of surveillance authorisation appear to be, with an authorisation to commence surveillance procedures being available without judicial scrutiny in both systems. However, if one delves a little deeper you will find that the Irish system, which is seen in this paper as a representative of the Anglo-American model, does not possess the same standards of privacy protection as are evident in Germany. This is felt most strikingly in the fact that the Irish Constitution has not developed a hierarchical determination as to what extent a person's privacy ought to be infringed in order that the greater good of investigating crime can be satisfactorily conducted. This paper asks for greater delineation in the system of privacy protection in Ireland with the German system offering an excellent basis upon which to proceed.

Many people may argue that the German model allows greater detail to be present in the theory of privacy protection and a person's ancillary rights, however this argument does not convince for the simple reason that the 'corn sphere' theory is based not upon a technical disposition of the old adversary v inquisatory debate, but upon the fundamental concept of what is meant as 'privacy' which goes to the centre of the philosophical underpinning of German society, which is central to that society. What is certain is that, in Ireland, the 2009 Act does not provide the necessary strategy to strike the correct balance between ensuring that privacy rights are protected, and that crime is also investigated, which means that alternatives must now be considered. This paper has offered an alternative process which Irish legislators may wish to consider in the future.