Cyber-crime, Confiscation, Disclosure, Mutual Legal Assistance, the Budapest Convention 2001, and Privacy Law In Ireland

Cybercrime may be defined, in Ireland, as any crime committed on the internet or electronically- such offences can include theft, or online fraud hacking of a computer, child pornography, child grooming, harassment, blackmail, drug trafficking, incitement to hatred.

An example of the use of technology to assist in criminal activity is the emergence of crypto markets on the dark net such as the Silk Road versions 1 and 2, and Agora market for the purchase and sale of illegal goods such as drugs, weapons etc, using virtual currencies such as bitcoins – see **Report of the European Centre for Monitoring Drug Trafficking and Drug Addiction January 2016.**

These types of markets are set up using websites such as Tor where an Administrator organises a new website for the sale of some illicit material who then takes orders from sub agents, who take orders from individuals or other criminals for drugs or guns etc. The majority of the transactions are paid for in bit coins or other virtual currencies which make them difficult for law enforcement agents to move against.

There is no criminal offence for "cyber crime" set by Irish Law. What is illegal in the real world is illegal in the cyber world. Mobile communication, computer and the internet has provided criminals with new means and methods of committing old traditional crimes.

It is believed that many crimes are committed on an extraterritorial basis. Australia has estimated that nearly 70% of its cybercrime is committed outside its territory which can cause problems in the investigation and apprehension of individuals.

Apart from crimes actually committed using the internet, or committed against computers or software (such as computer hacking), computer evidence and electronic footprints can be of great value to law enforcement agencies, and provide circumstantial evidence in relation to crimes which cannot be committed on cyberspace, such as murder and rape. There are a number of offences commonly associated by Irish law enforcement agencies with cybercrime and what follows is a brief discussion of some of these crimes.

Harassment

Section 10 of the Not Fatal Offences Against the Person Act 1997 provides that a person harasses if another person without lawful authority or reasonable excuse, by any means, including the use of the telephone, by persistently following, watching, pestering, besetting or communicating with another person resulting in a serious interference with that persons' peace and privacy or causing alarm, distress or harm to another.

There have been a growing number of cases over the last number of years where individuals have sent racist, threatening or abusive messages to each other over the internet or to friends, families work colleagues, or the public at large using the internet, or other electronic means such as twitter, or mobile phone technology. There has been some discussion as to how many times and how many people need to see such messages before the offence of harassment is committed. Irish Prosecutors will require, however, at least two clear incidents of harassment before a direction to prosecute is given because of the requirement of persistence. . It may be argued that leaving a derogatory

message or post on the internet for even a short time can mean that the alleged harassment is persistent. The Law Reform Commission has recently issues a discussion paper on the law of harassment which the office of the DPP has made a submission to.

Hacking

Hacking of a computer can cause computer webpages to be damaged or personal information can also be stolen. There have been a growing number of reported cases of commercial, political or non-governmental agencies whose computer systems have been hacked by computer activists in order to post messages that damage the reputational, political, or commercial objectives of those organisations, such as pre releasing online a number of movies belonging to major US film companies. This type of damage, which is often not made for personal gain, can be prosecuted in Ireland, using the provisions of section 5 of the Criminal Damage Act 1991.

The Irish Department of Justice on January the 20th 2016 published **the Criminal Justice (Offences Relating to Information Systems) Bill 2016**. The primary purpose of the bill was to transpose the European Directive 2013/40 or the Cybercrime Directive. The Directive is aimed at harmonising member states criminal law in the area of cybercrime by creating minimum rules for the definition of cybercrime offences and the relevant sanctions and to improve cooperation between competent authorities. The bill creates five key cybercrime offences namely:

- accessing information system without lawful authority (e.g. hacking)
- interfering with an information system so as to hinder or interrupt its functioning (e.g. introducing malicious software)
- interfering with data without lawful authority
- intercepting the transmission of data without lawful authority, and
- use of a computer programme, password, code or date for the purpose of the commission of any of the above offences.

The offences carry sentences of up to five years imprisonment on conviction on indictment. A tougher penalty of up to ten years imprisonment applies to the offence of interfering with an information system without lawful authority. Identity theft will be deemed to be an aggravating factor for sentencing purposes for the two data specific offences. It will also be an offence to obstruct a Garda acting under the authority of a search warrant (in relation to the investigation of a suspected offence under the act) or to fail to comply with a requirement given by such a Garda. Such an offence will be punishable by up to 12 months imprisonment or a class A fine (five thousand euros).

The bill allows for both territorial and nationality based jurisdiction. The key cybercrime offences may be tried in the state where the offence was committed in whole or in part by a person:

- in the state in relation to an information system outside the state;
- outside the state in relation to an information system in the state or
- outside the state to an information system outside the state where the act is an offence in the place it occurred and the person is an Irish citizen or is ordinarily resident in the state or is an Irish company.

Theft and Deception

E mail addresses may be hacked into in order to gain information about a person's financial details. Offenders can then send messages to their businesses or banks directing those firms to transfer sums of money to various bogus bank accounts. Alternatively elderly or vulnerable people may be contacted by individuals telling them about bogus safe investment opportunities or lottery wins for which they require their bank details for "administration fees or taxes " to be paid online before the injured parties received a dividend or prize.

Once the money is paid over of course, the bearers of good news or investment opportunities disappear.

Alternatively goods can be advertised on websites such as Done Deal or Gumtree for the sale of vehicles or machinery. These websites often advertise pictures of goods that are in fact copied from other sites. Arrangements are made online and by phone between bogus vendors and purchasers for the sale of these goods which of course are either non-existent or belong to other legitimate owners. When the goods are not delivered the injured party is at a loss often to the tune of thousands of euros. This type of action is criminalised by sections 4 (theft) and 6 (deception) of the Criminal Justice (Theft and Fraud offences) Act 2001 and by section 9 (use of a computer to make a gain or cause a loss) of the same Act.

Revenge Porn

Recently the phenomenon of "revenge porn" has begun to occur where sexually explicit visual material is posted online without the consent of the person portrayed. Such porn is often posted out of spite or retaliation by a jilted partner, although threats of blackmail and extortion can also occur. This type of activity appears to be on the rise particularly with the advent of inexpensive smartphone capability and the recent emergence of image sharing apps such as Instagram , Snapchat and Whats app. Ireland does not have specific statutory provisions to deal with revenge porn, and in the interim victims are obliged to seek injunctive relief, destruction orders, and damages by the use of pre digital laws such as privacy, defamation, data protection laws, and breach of confidence and or the emerging area of constitutional tort law as outlined by Hogan J in Sullivan v Boylan 2013 IEHC.

The right to privacy is also an un enumerated right as set out in Article 8 of the European Convention of Human Rights, although this might be tempered by Article 10 freedom of expression rights if this type of information was shared on a consensual basis initially. (See the paper given by Pauline Walley SC on Cyber Bullying/ Harrassment on 3rd March 2016 at the Office of the Irish DPP)

Child Pornography

The possession and distribution of child pornography, and the inducement of children below the age of 18 to engage in any pornographic or indecent act, or to induce them to engage in prostitution, or to advertise these children as being prostitutes is prohibited by the 1998 Child Pornography Act as amended. Using a computer to make online arrangements to travel to and meet children for the purpose of sexual activity is also prohibited by virtue of the 2008 Criminal Justice (Human Trafficking) Act.

Drug Trafficking

Section 15 of the Misuses of Drugs Act 1977 to 84 as amended criminalises the distribution or sale of prohibited substances such as cocaine, heroin or cannabis. The importation or export of these drugs into or out of this jurisdiction is also prohibited by the same legislation. Since 2009 there has been a growing emergence of crypto markets in the dark net net providing for the sale and purchase of drugs - often of substantial amounts - using virtual currencies such as bitcoins as the consideration for this type of activity. This type of activity is still a very small part of the general drug trafficking market but websites such as the Silk Road were still able to generate profits for their creators in the region of $60 million before they were closed down. When the drugs or weapons are being sent to the purchaser they are usually sent using the postal service either to the purchaser himself or to a place where he can collect them.

Law Enforcement Measures Against Cybercrime

As the definition of cybercrime involves the commission of crime in the real world, the tools for the confiscation of the benefits of those crimes are the same as in the real world. There are particular issues however in connection with retaining, obtaining, proving, and disclosing evidence relevant to cybercrime investigations. One of the many issues that has arisen in connection with cybercrime activity is how to identify the suspected criminal in many of these cases, then prove electronic evidence obtained as a result of the investigation, and if convicted confiscate or forfeit any benefit those persons obtained as a result of the crimes which they are convicted of. I will deal with the issue of confiscation and forfeiture first.

Confiscation and Forfeiture

The Irish Law Enforcement Authorities can avail of two statutory forms of criminal confiscation/forfeiture: conviction based, and non- conviction based. The Criminal Assets Bureau can obtain forfeiture orders in relation to property that can be proven on the balance of probabilities to be associated with criminal activity using the freezing and disposal order process provided for under the Proceeds of Crime Legislation 1996 to 2005. The Criminal Assets Bureau is also the nominated Assets Recovery Office for Ireland for the purpose of international co-operation in EU international investigations into the Proceeds of Crime.

The Bureau is also a member of the CARIN network of Assert recovery units in various different countries which include many countries outside the EU. The Bureau has as part of its staff complement a computer forensic analyst who can assist in criminal investigations of the dark net.

The Office of the DPP deals with the remedies for criminal asset confiscation provided for under the Criminal Justice Act 1994, and the Criminal Justice Mutual assistance Act 1994. If cybercrime offences are connected to drug trafficking, or money laundering offences whose predicate offences are connected to drug trafficking, then the DPP can apply for a court based enquiry into any benefit obtained by any person convicted on indictment as a result of those offences pursuant to section 4 of the Criminal Justice Act 1994, and as provided for by section 117 of the Criminal Justice (Money laundering and Terrorist Financing act) 2010.

There are statutory presumptions provided for in such cases under section 5 of the 1994 Act, allowing the court to assume that any assets generated by the defendant for six years prior to the commencement of criminal proceedings against him were generated as a result of drug trafficking

activity. The onus is placed on the Defendant to prove otherwise and the standard of proof is the balance of probabilities.

For any other offence tried on indictment the prosecution must prove that the benefit gained by the Defendant was obtained as a direct result of the offence for which that person was convicted, - see section 9 of the Criminal Justice Act 1994 as amended. Thus if 50,000 euros was seized in a theft offence then only 50,000 euros can be ordered to be confiscated.

As most online theft offences involve innocent parties it would be appropriate to seek a restitution order pursuant to section 56 of the Criminal Justice (Theft and Fraud) Offences Act 2001 in relation to any property still identifiable and in the possession of the Defendant or his agents. Such orders can also be executed abroad if the relevant property can be located and frozen there pursuant to section 84 of the Criminal Justice (Mutual Assistance) Act 2008.

Freezing, Forfeiture, and confiscation orders obtained post- conviction in this jurisdiction can also be executed abroad using sections 33, 49 and 58 of the 2008 Criminal Justice (Mutual Legal Assistance) Act. Property owned, controlled or transferred to third parties for below market value by defendants can be frozen prior to, or post conviction using section 24 of the Criminal Justice Act 1994 or section 33 of the Criminal Justice (Mutual Assistance) Act 2008.

Incorporeal property such as domain names for websites can also be forfeited pursuant to section 61 of the Criminal Justice Act 1994 or in a confiscation enquiry, and closed down with the cooperation of service providers. Domain names and telephone numbers have been confiscated in the past for cases involving the organisation of prostitution.

Evidence located abroad can also be sought to be frozen pursuant to section 32 of the 2008 Criminal Justice (Mutual Assistance) Act. Account monitoring orders for accounts abroad can also be obtained by An Garda Síochána pursuant to sections 17 and 18 of the 2008 Act.. An Garda Síochána may also seek to freeze accounts in this jurisdiction pursuant to section 17 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.

A certificate is required to be issued by the courts of the relevant jurisdiction before courts in the EU will freeze evidence property in their own jurisdiction despite the fact that provision is also made for spontaneous communication between relevant competent authorities in various jurisdictions both under the various conventions dealing with mutual legal assistance and our own 2008 Act. Most states in Europe still refuse to recognise non conviction based forfeiture orders except on an ad hoc case by case basis.

The problem with many on line frauds is trying to find and trace the destination of stolen property once it is transmitted to bogus accounts. Criminals may use "mules" to collect money from bogus accounts for them even where organisations such as Western Union require the names of the persons who collect the money. And despite pending legislation re beneficial ownership of companies and bank accounts the information provided by criminals and their agents to banks, property registration authorities, or company offices may be false.

In the recent case of **DPP -v Ezenwatu Izundu 2014 IEHC** Judge Barrett in the High Court indicated that the trial court in a confiscation enquiry was obliged by section 6 of the Criminal Justice Act 1994 to make a finding as to whether assets were realisable. Judge Nolan in the lower Circuit Trial Court interpreted this to mean that the prosecution must carry out further investigations into the locations where funds are transmitted in other jurisdictions in order to prove that the

defendant had hidden the relevant assets, despite the fact that the case law in the past had reversed the burden of proof on the defendant to show that he had not hidden those assets.- (**Phillips v UK ECHR 5th July 2001 , DPP-v- John Gi**lligan Special **Criminal Court 22nd March 2002 , and R-v- David Comiskey UK court of Appeal 1990-**91 12 **CR. APP. P(s) 412ase)** Where the defendant had transferred the assets onto another country outside the EU it may be impossible to carry out further investigations and the limits of this type of confiscation enquiry are still being developed by the courts.

Extraterritorial Effect of Cybercrime

Lotus (France v Turkey (1927) PCIJ Rep Series A, N 10 –

"It is I certain that the courts of many countries even of countries that have given their criminal legislation a strictly territorial character, interpret criminal law in the sense that offences, the authors of which at the moment of commission are in the territory of another state, are nevertheless to be regarded as having been committed in the national territory if one of the constituent elements of the offence and more especially its effects have taken place there."

This issue has been addressed in relation to other offences e.g. sexual offences committed outside the jurisdictions by Irish citizens such as the Sexual Offences (Jurisdiction) Act 1996 Child trafficking and Pornography act 1998, Criminal Damage Act 1991, and the Criminal Justice (Money Laundering and Terrorist Finance) Act 2010 and the new Cybercrime bill 2016. A similar provision needs to be included in the 1997 Non-Fatal Offences Against the Person Act in relation to Harassment offences It has been suggested that where cybercrime exists in its various forms then a specific form of legislation should be required to indicate that where acts involving acts of cybercrime are committed (and a definition should be given as to what is meant by cybercrime) either in this jurisdiction, or outside it, that they are deemed to be criminal offences and will be penalised under Irish law The 2016 Act to a certain extent goes some way to doing this, but only in relation to interference with computers and information systems- it does not deal with many of the other offence referred to above.

Budapest Convention on Cybercrime 2001

The convention was the first international treaty on crimes committed via the internet and other computer networks dealing particularly with infringement of copyright, computer related fraud, child pornography, hate crimes and violation of network security. Ireland has signed the convention but not ratified it yet.

The convention also contains a series of measures and procedures dealing with areas such as the search of computer networks and lawful interception. Its main objective, as set out in the preamble, is to pursue a common criminal policy among its parties aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.

The convention aims principally at:-

- harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber crime

- providing for domestic criminal procedural law powers necessary for the investigation and

prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form

- setting up a fast and effective regime of international cooperation

The following offences are defined by the contention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer related forgery, computer related fraud, offences related to child pornography, and offences related to copyright and neighbouring rights.

It also sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production orders, search and seizure of computer data, real time collection of traffic data, and interception of content data. The convention contains a provision on a specific type of trans border access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the signatory states. The 2016 Cybercrime bill still does not provide for speedy assistance between signatory states.

Computer data is defined as meaning any representation of facts, information, or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function.

Service provider is defined under the convention as any public or private entity that provides to users of its services the ability to communicate by means of a computer system, and any other entity that processes of stores computer data on behalf of such communication service or uses of such service. Traffic data means any computer data relating to a communication by means of computer systems, generated by a computer system that formed a part in the chain of communication , indicating the communication's origin, destination, route, time, data, seize duration or type of underlying service.

By virtue of article 15 each party is obliged to ensure that the establishment, implementation, and application of the powers and procedures provided for in the convention are subject to conditions and safeguards provided for under its domestic law, and which shall provide for the adequate protection “of human rights and liberties including rights pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.”

The article goes on to state that to the extent that it is consistent with the public interest, in particular the sound administration of justice, each party shall consider the impact of the powers and procedures in the convention upon the rights responsibilities and legitimate interests of third parties.

Article 16 provides that each party shall adopt “such legislative measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. “The parties to the convention are obliged to require service providers to preserve the data “as long as is necessary up to a maximum of ninety days to enable the competent authorities to seek its disclosure. - such order can be subsequently renewed”.

Each party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

Article 17 provides that the parties to the convention shall adopt in respect of preserved data under article 16 such legislative and other measures as may be necessary to ensure that such data is available regardless of whether "one or more service providers are involved in the transmission of that communication" and ensure the expeditious disclosure to the party's competent authorities of a sufficient amount of traffic data to enable the party to identify the service providers and the path through which the communication was transmitted.

Article 18 provides that when a production order is served " a service provider offering its services in the territory of the party to submit subscriber information relating to such services in that service provider's possession or control " although such powers and procedures must be subject to the limitations outlined in article 15.

Article 19 obliges parties to adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access a computer system or part of it ,and computer data stored therein and a computer data storage medium tin which the computer data may be stored in its territory.

Where the data is "lawfully available to the initial system" the authorities shall be able to expeditiously extend the search or similar accessing to the other system" subject to the provisions of the domestic criminal law and the fundamental rights outlines in article 15.

Article 22 provides that each state signatory shall adopt such legislative measures to ensure that any offence established in accordance with the convention to establish jurisdiction when the offence is committed on its territory, on board a ship flying the flag of that party, or on board a plane registered in the state, or by one of its nationals if the offence is punishable under the criminal law where it was committed, or if the offence is committed outside the territorial jurisdiction of any state. Where more than one party claims jurisdiction over an alleged offence established in accordance with the convention the parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Article 25 provides that the parties shall extend the maximum possible mutual assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data or for the collection of evidence in electronic form, of a criminal offence subject to the usual rules about dual criminality and grounds for refusal.

The Convention was acceded to by the United States in 2006 and signed by Canada, South Africa as well as Australia, Dominican Republic, Japan , Mauritius , Panama, Some countries outside the Europe have not acceded to the Convention including China, Russia and India. One of the reasons given by these countries for not signing the convention was because they were not involved in its preparation and negotiation. There have been indications that some countries do not wish to join the convention because of its strictures relating to copyright law. There may be difficulties was well in getting some countries joining a global convention on cybercrime as there have been allegations that some countries might use such a convention to assist in investigations in relation to internal dissent.

Powers of Investigation in relation to Cyber Crime under Irish Law

Under Irish Law a valid search can be conducted of a person or property (or both) in four discrete circumstances:

i) where the person consents to the search

ii) where there is a valid search warrant

iii) on foot of a valid arrest or

iv) pursuant to specific statutory powers .

In most cases a search warrant will be required before a search can be carried out. However a search of premises consequent on lawful entry for the purpose of arrest does not require a warrant.

There are hundreds of statutory provisions dealing with search warrants. Some can be issued by a court, some by a peace commissioner and some by a member of An Garda Síochána not below a certain rank, some by Revenue officials. Some must be executed within a few days, some in a week, some can be executed in a month. See section 16 of the Criminal Assets Bureau Act 1996 and section 14 of the Criminal Justice Drug Trafficking Act 2001.

Certain regulatory statutes give the Gardaí power to enter without warrant and take away certain specified items. These statutes apply to a variety of premises such as those used for the slaughter of animals, pawn broking, and the sale if illicit liquor. Reasonable suspicion of a criminal offence does not have to be present in these cases in order to enter pursuant to these statutes. A separate class of statutes permit entry without warrant on reasonable suspicion of a specified offence such as the possession of explosives or chemicals weapons, the health and welfare of a child, and drug trafficking. An Garda Síochána may detain a person for a reasonable period without deciding to affect an arrest. However if the search reveals incriminating objects the Gardaí must arrest and charge the person.

Section 5 of the Criminal Justice Act 2006 provides that a member of an Garda Síochána not below the rank of Superintendent may designate a place as a crime scene where he has reasonable grounds for believing either that an arrestable offence has been or is being committed in that place or that there may in the place evidence relating to an arrestable offence committed elsewhere, and it is necessary to designate the place as a crime scene to preserve, search for, and collect evidence of or relating to the commission of this offence. Section 5 (4) states that any direction designating the place a crime scene may also permit entry and search of that place for evidence and the preservation, search or collection of any such evidence A direction under section 5 remains in force for no longer than is reasonably necessary to preserve, search for, and collect the evidence concerned.

Section 5(7) states that such direction in relation to a place other than a public place shall cease 24 hours after it is given. There is provision for the extension of the direction by the District Court, and subsequently by the High Court.

Members of An Garda Síochána have a common law right to seize evidence found in the course of a lawful search irrespective of whether or not such evidence is related to the purpose of the search.

In Jemmings v Quinn O'Keeffe J outlined the extent of police powers of search and seizure on foot of a lawful arrest. The Gardaí may take evidence in support of the crime for which the arrest was made and evidence in support of any other offence that might be contemplated against the person or evidence reasonably believed to be stolen property, or unlawfully in the possession of the person.

This power was recognised and extended by section 9 of the Criminal Law Act 1976 which states that where in the course of a Garda Search carried out under any power, a member of an Garda Síochána, a prison officer, or a member of the Defence forces, finds or comes into possession of anything which he believes to be evidence of any offence or suspected offence, this may be seized and retained by him for use as evidence in any criminal proceedings for such period from the date of seizure as is reasonable . Section 7 of the Criminal Justice Act 2006 extends this power of seizure to evidence found in a public place or in the course of a consensual search.

Other miscellaneous statutory provisions serve to consolidate this position. For example s 10 (3) (C) of the Criminal Justice (Miscellaneous) Provisions Act 1997 specifically provides that anything found at the place named in a search warrant issued pursuant to the act, or found on a person at that place may be seized if reasonably believed to be related to an arrestable offence. (an offence carrying a possible penalty of at least five years) The word "anything" is wide enough to cover electronic evidence.

Similarly section 27(2) (C) of the Electronic Commerce Act 2000 provides for the seizure of electronic evidence obtained as a result of such a search. When the item seized contains information or an electronic communication that cannot readily be accessed or put into intelligible form, section 27 grants the power to compel the disclosure of the information or electronic communication in intelligible form.

Evidence obtained as a result of a production or access order

In certain limited circumstances statute permits the making of production and access orders against third parties, who, although not suspected of a crime, are believed to be in possession of information relevant to the commission of a criminal offence.

Section 63 of the Criminal Justice Act 1994 as amended by section 105 of the Criminal Justice (Mutual Assistance) Act 2008 permits a member of An Garda Síochána to apply for a production or access order in respect of material which he or she has reasonable grounds for suspecting is of substantial value to the investigation into drug trafficking or money laundering. Such an order will only be granted by a court if there are also reasonable grounds for believing that it is in the public interest that the material be produced. Such orders do not extend to material protected by legal professional privilege. Where a production and access order is impracticable s. 64 permits the making of a search warrant in lieu.

Section 52 of the Criminal Justice (Theft and Fraud Offences) Act 2001 also makes provision for the issue of production and access orders where there are reasonable grounds for suspecting that a person has possession or control of material which constitutes evidence of or relating to the commission of any offence under the Act punishable by imprisonment for a term of five or more years or a more severe penalty.

Section 15 of the Criminal Justice Act 2011 allows the Gardaí to apply to the District Court for an order requiring a person to produce documentation within the criteria set out in section 15 (2) (Aar) (3) (b) -(d).

Section 6 of the Communication (Retention of Data) Act 2011 also enables a Garda Síochána, members of the Defence Forces and Revenue officials to make a disclosure request to obtain access to retained data.

The trend in these statutes dealing with electronic evidence is to progress from just obliging person in control of such information to provide passwords or raw data to actually explaining the information in question and also put it into intelligible form- see sections 48 and 52 of the 2001 Criminal Justice (Theft and Fraud Offences) Act, the Criminal Justice Act 2011 and the Cybercrime Bill 2016.

Surveillance and the Right to Privacy

The existing case law of the Irish Superior Courts contains clear statements of a constitutional right of privacy and the freedom from unjustified surveillance. None the less the contents and limits of that right are unclear and do not permit the citizen, the media or others concerned to determine clearly what their rights or obligations are in that sphere.

The courts have on occasion been willing to permit overt surveillance by members of the police force. The crucial consideration in such cases is whether the nature of the surveillance concerned is in breach of the person's constitutional rights. The Irish courts have distinguished between **overt** and **covert** surveillance. In **Kane v Governor of Mountjoy Prison 1988 IR 75** the applicant was the subject of intense and constant surveillance by the police having been released from prison. The guards were aware that the applicant was the subject of an extradition warrant and rearrested him on his release. The Supreme Court found that the surveillance could only be lawful if it could be justified. Finlay CJ was not willing to endorse any general application of such a procedure by the police, and instead insisted upon a specific and adequate justification for its use. McCarthy J dissenting in part indicated that covert surveillance differed from overt surveillance in that in the former the subject's freedom of choice of movement was restricted. In addition it was pointed out that Gardaí may lawfully "stake-out" premises they believed would be burgled. Finally when the police sought to detect crime they could follow a suspect overtly or otherwise.

In the case of **Kennedy v Ireland 1987 IR 187** the phones of a number of journalists were tapped on the orders of the then Minister for Justice who admitted that there was no direct justification for doing so. The Supreme Court held that the constitution provided a right to privacy which included the right to hold private telephone conversations without deliberate, conscious and unjustified intrusion. This right could legitimately be restricted in the interests of public order, public morality, and the common good, as well as to protect the constitutional rights of others. In the instant case the absence of such justifying factors resulted in the court finding that the plaintiffs' constitutional rights had been infringed.

In **DPP v Dillon 2002 4 IR 101** the applicant challenged the admissibility of certain mobile telephone evidence in his trial. Statute prohibited the interception of telecommunications messages unless the interception was authorised by the Minister for Justice for the purposes of a criminal investigation. The Court of Criminal Appeal found that listening to a telephone conversation without the agreement of the caller was unlawful where evidence of the record made was intended to be introduced in a criminal trial. The court of Criminal Appeal at a later date questioned the correctness of this approach in **Geasley v DPP 24 March 2009** to the extent that it focused on the agreement. The Court noted that the term agreement has been referred to in section 98(5) of the Postal Communications Act 1982 which had been replaced by section 13(3) of the Postal Packets

and Telecommunications Messages (Regulations) Act 1998 and as a result it was not unlawful for a person to receive a message from another person where that person does not consent to being listened to or recorded.

In November 2014 the Minister for Justice and Equality signed a statutory instrument bringing into effect Part 111 of the **Criminal Justice (Mutual Legal Assistance) Act 2008** whereby designated states can seek interception of telephone and certain email and text services in Ireland for the purpose of criminal investigations. The evidence may be used in criminal prosecutions as well. Similarly Irish law enforcement agencies can seek telecommunications and internet intercepts in relation to data that is being generated abroad on foot of an Irish investigation. Service providers who refuse to comply with a warrant may be required to appear before an in camera hearing of a tribunal. The services may not disclose their objections to the tapping of telecommunications or texting or certain email services. This particular point may be open to judicial scrutiny in the future.

There has been controversy recently when GSOC (Garda Ombudsman's Office), which was set up by the Garda Síochána Act 2005, used its powers of investigation in relation to tapping (it has the same powers of investigation as an Garda Síochána and in 2015 the Garda powers for surveillance were extended) journalists' phones. The use of this power by GSOC is being investigated by an inquiry chaired by the former Chief Justice Mr Murray.

In terms of video surveillance the courts have indicated that where the recorded footage contains nothing more than would be observed by an onlooker there is no objection to this evidence being admitted in the course of a criminal trial **Atherton v DEPP (2005) ID**EC The finding might be different if the setting up of the surveillance involved trespass onto private property.

The **Criminal Justice (Surveillance) Act 2009** provides that a judge of the District Court, upon application by a member of an Garda Siobhan not below the rank of Superintendent may issue an authorisation which permits surveillance to be carried out where there are reasonable grounds for believing that the surveillance is necessary for obtaining information in relation to the commission of an offence, or the prevention of the commission of an offence. The superior officer must also have reasonable grounds for believing that the surveillance is proportionate to its objectives, and the least intrusive means possible having regards to those objectives. The Act also allows the carrying out of surveillance without authorisation in cases of emergency. Section 8 entitles a member of the Gardaí, Defence Forces, or Revenue Commissioners to monitor the movements of persons, vehicles or things using a tracking device if that use has been approved by a superior officer. Judicial authorisation of such devices is not required.

The European Convention on Human Rights determined in the case of **Uzon v Germany (2010 53 EHRR 85**2 that GPS surveillance by its very nature is to be distinguished from other methods of visual or acoustical surveillance which are as a rule more susceptible to interference with a person's right to respect for private life, because they disclose more information on a person's conduct, opinion or feelings.

It is clear from the case of **Curtin v the Clerk of Dáil Éireann 2006 IESC** that the failure to observe the constitutional rights of the accused may result in the inadmissibility of electronic evidence. In that case a judge was charged with possession of child pornographic material. The guards however had seized his computer using an out of date warrant. He was therefore acquitted of the charges as the evidence on the computer was deemed to be inadmissible.

In 2012 the Supreme Court in the **Damache v DPP (2012 IESC)** ruled that a search warrant issued

pursuant to section 29 of the Offences against the State Act 1939 by a Superintendent of Mr Damache's house to be invalid. Denham J ruled that a Superintendent who authorised the warrant was not independent of the investigation, and was therefore not able to assess the conflicting interests of the state and the individual person. The search warrant was also for the Mr Damache's dwelling house, and the constitution in article 40.5 expressly provides that the dwelling is inviolable and shall not therefore be forcibly entered save in accordance with law "which means without stooping to methods which ignore the fundamental norms of the legal order postulated by the constitution. Entry into a home is at the core of potential state interference with the inviolability of the dwelling".

This decision led to a number of convictions obtained on the basis of evidence obtained as a result of section 29 warrants being overturned – see **DPP -v- Timothy (Ted) Cunningham, and DPP -v- Jason Kavanagh Mark Farrell and Christopher Corcora**n. New legislation provided that members of an Garda Siobhan below a certain rank could issue warrants provided that they must be independent of an investigation, and they must issue warrants only in the case of emergency, and also in normal course applications should be made to a court for such warrants.

A further development in this corpus of law was the case of **DPP v JC (Supreme Court 15th of April 2015)** where the guards had used a section 29 warrant to enter a house and arrest JC in a burglary case. Mr JC was detained and made inculpatory statements. Three days later the Supreme Court Judgement in Damache was handed down, and an application was made to the court trying Mr JC to exclude the evidence obtained as a result of the section 29 warrant. The trial Judge, applying the ruling of **DPP v Kenny** excluded the evidence, and the trial against JC collapsed. The Director appealed the decision to the Supreme Court, and by a four to three majority the Supreme Court ruled that the Circuit Court Judge was erroneous.

Judge O'Donnell, for the majority, which included Judge Denham, ruled in April 2015 that because the guards in obtaining the warrant had inadvertently applied for the warrant pursuant to the wrong section, the mere fact of this inadvertence, where the interference with the constitutional rights was not deliberate or conscious, did not automatically invoke the exclusionary rule as to evidence as enunciated in the Kenny Decision.

Judge Hardiman for the minority, in a very strong dissent, said that he was horrified with the majority decision, and indicated that in the light of various tribunals of inquiry into Garda misbehaviour that it would be very unwise to have overturned the exclusionary rule as laid down by Kenny and to give an Garda Síochána "effective immunity" from judicial oversight which this case did. This decision in effect reversed the previous decision of the Supreme Court in **DPP v Kenny 1990 2 IR** where a guard had applied for a search warrant but there was no evidence that the court had investigated the reasonableness of the suspicion grounding the application for the warrant. The Supreme Court held in that case that the search warrant was invalid and that even though there was no deliberate or conscious violation by the police of the defendant's rights any evidence obtained on foot of such a warrant could not be admitted except in the most exceptional circumstances which were elaborated on.

Does Judicial Oversight Provide Sufficient Privacy Protection?

Dr T. J McIntyre in his paper on Judicial Oversight of Surveillance published in 2016 has argued that there is an ongoing debate as to what role the judiciary should play in relation to surveillance and oversight in the collection and retention of data by independent institutions Dr McIntyre has pointed out that in the European Court of Human Rights case (ECTHR) case **Klass v Germany the**

ECTHR a**pplication 5029/71** 6 September 1978 paragraph 55 expressed a strong preference for judicial control at the point where surveillance is first ordered, and while it is being carried out stating that "in a field where abuse is potentially so easy in individual cases, and could have such harmful consequences for democratic society as a whole it is in principle desirable to entrust supervisory control to a judge "

Dr McIntryre has noted however that the UN Commissioner for Human Rights has concluded that "judicial review of digitial surveillance activities, or intelligence, and or law enforcement amounted effectively to an exercise in rubber stamping. The Commissioner recommended a mixed model which would combine administrative, judicial and parliamentary oversight."

Dr McIntyre's article has argued that the need for independence and detachment reflects the conflicting incentives of the police and intelligence/security agencies who are institutionally unlikely to give adequate weight to privacy concerns. The article continues that this is particularly important in the context of terrorism, where experience has shown that the executive and legislature can be prone to overreactions.

Alternatively it has been argued that the judiciary are removed from the political cycle, and as they are less directly influenced to popular opinion, they are best placed to consider whether measures "which appear desirable in the short term are in accordance with the law and – in the last resort whether they are compatible with the longer term interests of a democratic society."

At the same time Dr McIntyre has noted that while some specialist judges may acquire expertise in examining whether surveillance should have been authorised (he notes the establishment of the US Foreign Intelligence Surveillance Court) "these in turn present their own risk of regulatory capture as a small pool of judges hearing only from the security agencies who may come to lose their objectivity"

Dr McIntyre has argued, therefore, that it is therefore important that judicial controls should not exist in isolation but should form part of a wider system of accountability including specialist oversight institutions.. He went on to note that the report from the Venice Commission "Report on the Democratic Oversight of the Security Services" have recommended that such systems must cover all aspects of the work of intelligence agencies including the interaction between difference agencies and the police. Systems which focus on particular instances of surveillance may overlook other threats to privacy such as data mining or the sharing of intercepted communications with other countries.

Dr McIntyre examined judicial supervision provided prior to surveillance taking place, and after the fact (ex ante and ex post). He has argued that ex ante judicial control will be most effective at safeguarding rights if it involves the application of clear and well defined rules. Where open ended laws are involved he has argued that there is a risk that a secret body of case law may develop outside the adversarial process, without scrutiny by appellate courts or the wider legal community.

Dr McIntyre also noted that Ex post judicial oversight also varies greatly between national systems. A common form is judicial examination of complaints that an individual has been wrongfully subjected to surveillance whether through the courts or a specialist tribunal. Dr McIntyre while acknowledging this as an important remedy it has the disadvantage of being reactive in nature and dependent on the individual being aware of the surveillance, and being able to access evidence proving abuse, and therefore works best in systems which provide "for individuals to be notified after surveillance has ceased". Another example of ex post scrutiny is where intelligence is

challenged when it is sought to be introduced as evidence in a criminal trial. Dr McIntyre has argued this is a weak form of scrutiny as it is ad hoc in nature and does not disclose possible wider forms of abuse ie where surveillance is carried out by security services and where it is thus unlikely that any particular case will end up in court .

The doctor has pointed to a series of cases have developed under European Human Rights Law which have identified a set of issues which must be addressed in legislation In Weber and Saravia v **Germany Application 54934/00 29 June 2006 par 94** the following minimum safeguards were set out by the ECT HR in relation to secret measures surveillance (in this case telephone surveillance):-

a) the nature of the offences to which the surveillance apply must be clear:-

b) there must be a definition of the categories of people liable to have their telephones tapped

c) there must be a limit to the duration of telephone tapping

d) there must be a clear procedure for examining using and storing the data obtained

e) precautions must be taken in communicating the data to other parties

f) the circumstances in which recordings may or must be erased or the tapes destroyed must be set out.

g) The laws governing such surveillance must provide an adequate and effective remedy against abuse.

Where other rights which might be interfered with by the surveillance are specifically protected under the Convention, such as communications between lawyers and clients, or communications between journalists and their sources, the case law appears to call for ex ante judicial supervision.

In Klass v Germany the court stated that given the special dangers of secret surveillance effective control should normally be ensured by the judiciary indicating that the individual should ultimately have the ability to bring an action before the courts which Dr McIntyre argues means that ultimately that the individual should be made aware of measures taken without his knowledge and thus able retrospectively to challenge their legality.

In **Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria application** 62540/00 the principle of notification was summarised as being “as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned.”. The decision appears to treat subsequent notification as a mandatory requirement.

Article 52 of the **EU Charter of Fundamental Freedoms** (in force since the treaty of Lisbon 2009) states that in so far as the EU Charter contains rights which correspond to the European Convention on Human Rights, the meaning and scope of those rights shall be the same as laid down by the said convention. In essence this means that the EU court of Justice will also apply ECTHR law. The ECTHR decisions may be implemented years after rulings are handed down (It took Ireland many years to decriminalise homosexuality after the ECTHR handed down a ruling holding that it was incompatible with the contention). Rulings by the EU court of Justice however

are immediately applicable as EU law under article 28 of the Irish Constitution and superior to the rulings handed done by the Irish Supreme Court in this area of jurisdiction

In the Digital Rights Ireland case discussed below the Courts of Justice of the European Union found that the EU Data Retention Directive was disproportionate in its scope. The court found that one of its most significant faults was the lack of ex ante judicial or quasi judicial approval before retained date could be accessed by Law enforcement agencies. The question arises as to whether this decision will apply to Irish domestic legislation on data retention. In the Irish context one of the more important pieces of legislation for Law Enforcement purposes in relation to investigating crime is the Communications (Retention of Data) Act 2011

The Communications (Retention of Data) Act 2011

The purpose of the 2011 Act is to allow for the retention and retrieval of specified data held by providers of fixed telephony mobile telephony and internet services. The Act gave effect to the Directive 2006/24 on the retention of data generated or processed in connection with the provision of publicly available electronic communications service of public networks.

Section 3 imposes an obligation on service providers to retain non content data such as IP addresses for two years for telephonic data, and one year for internet data from the date the data was first processed.

By virtue of the provisions of section 6 of the 2011 Act a member of an Garda Síochána not below the rank of Chief Superintendent may request a service provider to disclose to that member or officer data retained by the service provider in accordance with section 3 where that member or officer is satisfied that the data is required for the prevention, detection, investigation, or prosecution of a serious offence, the safeguarding of the security of the state, the saving of human life or the prevention, detection, investigation, or prosecution of a revenue offence.

Section 6 (4) of the Act provides that a disclosure request must be made in writing - in cases of exceptional urgency however the request can be made orally.

In **Digital Right Ireland Ltd v Minister for Communications Marine and Natural Resources (C-293/12) (2014) 3 WLR 1607** the Grand Chamber of the ECJ struck down the 2006 directive on the retention of data. The Irish Plaintiffs formed a limited company that bought a mobile phone and then issued proceedings in the High Court in Ireland claiming that certain rights which could be exercised by a limited company in Ireland were been infringed upon by the Directive.

The ECJ was called upon to examine the validity of the directive in particular in the light of two rights under the Charter of Fundamental Rights of the EU, namely the fundamental right to respect for private life, and the fundamental right to the protection of personal data. In April 2014 the Court of Justice concluded that the Directive was in breach of and was a disproportionate interference with the EU charter of Fundamental Rights Article 7 (right to private life) and Art 8 (protection of data). The court held that the directive was too wide ranging resulting in serious interference with private rights, while failing to show that such interference was limited to what was strictly necessary. In short it failed a proportionality test.

Article 29 of the Irish Constitution provides that no provisions of the constitution can be invoked so as to invalidate laws, measure etc. enacted and adopted as having been necessitated by our membership of the EU As the directive has been struck down by the ECJ the question arises as to whether the 2011 Act still retains constitutional protection under Irish law and also whether the ECJ will go on to rule in two further cases taken by the United Kingdom and Sweden that such domestic legislation must also be subject to compliance with articles 7 & 8 of the Charter or are otherwise invalid.

In the Irish Prosecution of a murder **DPP –v- Graham Dwyer** an Garda Síochána received essential CDR evidence (telephonic evidence) using the provisions of the 2011 Act in their investigation, and the prosecution subsequently at trial sought to admit into evidence the same evidence.

The CDR evidence consisted of mobile phone data showing the location of particular mobile phones, the contact made between such mobile phones, and the connected payments or subscriber details to show the location of the Defendant at particular times when he was in contact with the injured party. The Defendant challenged the admissibility of such evidence on the grounds of the ECJ Digital Rights judgement which struck down the 2006 directive. The Defence pointed out that the purpose of the 2011 act was to transpose the Directive into Irish Law. The trial Judge ruled that the electronic evidence was admissible in the case notwithstanding the ruling in the Digital rights case The Judge stated that the 2011 Act did not import any new requirement or concept into Irish Law . He held that the purpose of the 1996 directive was primarily directed towards commercial concerns, and that the EU was essentially trying to level the playing field for transnational operators.

The Directive imposed an obligation on member states to put in place data retention and access regimes. In this case Ireland already had such a regime courtesy of the Criminal Justice Terrorist Offences Act 2005 which was replaced by the 2011 Act. The second purpose of the Directive was to harmonise what retention and access regimes the member states had in place which the 2011 Act did. In relation to the 2011 Act the Judge stated that while the title of the Act indicated that it was to give effect to the Directive, it was also concerned with a number of other purposes such as the safeguarding the security of the state and the saving of human life. The 2011 Act unlike the directive did place a number of conditions and restraints on the retention of data including an appeal process.

The Judge held that even if the constitutional rights of the individual had been infringed the court could not elevate such an infringement to the status of a breach of any constitutional right of the defendant The Judge indicated that if he entered a bank he could be seen on cctv which has been seen already to have been sanctioned by the Irish Supreme Court in that it is an observation or overt surveillance that does not affect the internal privacy or feelings of the individual concerned, but is something that can be easily observed by anyone in the course of a normal day's activity.

The contents of the telephone messages were not relied on by the prosecution but the evidence showing his movements were which did not interfere with any core privacy right of the the Defendant. .

The court went on to rule that in light of the JC decision the court still had a discretion as to whether to allow the data on the basis that the guards believed that they had a statutory right to seek the information in question at the time they sought it.

This decision by the trial Judge is being appealed to the Court of Appeal.

While the 2011 Act contains a number of safeguards in addition to those expressly contained in the Directive, for the most part the Act closely mirrors the provisions of the Directive.

The Irish Data Protection Commissioner audited an Garda Síochána and issued a report on its procedures re accessing telephonic data in 2014 which has been published online. The report noted that an Garda Síochána had established a single contact point for requests for data in its Telecommunications Unit, and outlined to the investigation team its criteria when making a request for communications data:-

1. Where An Garda Síochána legally covered,
2. Could an Garda Siochana demonstrate relevance,
3. could an Garda Siochana demonstrate necessity
4. Is the data being sought proportionate e.g. not all traffic data at 6 am in central Dublin – narrow down the request further.

An Garda Síochána referred the Data Protection Commissioner to the oversight procedures in place based on the legislation, namely the annual review and examination of requests by a Judge to ensure all data sought by An Garda Síochána was sought legitimately within the confines of the legislation.

An Garda Síochána also sought certain information under the Data Protection Legislation 1988 as amended section 8. The ODP pointed out that this provision is permissive only, and it does not place any obligation on data controllers to provide An Garda Síochána with personal data. The report went on to state that the ODP considered that the key difference between the Communications (Retention of Data) Act 2011 and section 8 (b) of the Data Protection Act is that the former provides for mandatory disclosure where serious offences are concerned. The latter allows for voluntary disclosure subject to consideration on a case-by-case basis as to whether not releasing the data would be likely to prejudice any attempt by organisations which have crime prevention or law enforcement functions to prevent crime or to catch a suspect.

An Garda Síochána confirmed that they would seek to rely on section 8(b) of the Data Protection legislation for all data sought in relation to non-serious crime requests. The Office of the Data Protection Commissioner indicated that it would engage further with An Garda Síochána in order to develop an issue sectoral advice to all telcos in this regard.

An Garda Síochána review 10% of all requests every three months to see whether they are valid requests under the 2011 Act and a number of these requests were refused internally. Overall the Office of the Data Protection Commissioners was satisfied with the procedures in place although the auditors advised that all requests have to be signed by a Chief Superintendent.

During the Inspection a telecommunications company indicated that when processing a data subject access request made under section 4 of the Data Protection Acts it would not provide to the requesting data subject any information relating to requests that may have been made to it by An Garda Síochána under the 2011 act The Office of Data Protection advised the company that requests for disclosure from An Garda Síochána, Revenue or the Defence forces should be considered for release as part of a section 4 access request and should only be withheld if An Garda Síochána, the Revenue Commissioners, or the Defence forces confirm that release would prejudice the investigation, prevention, or detection of a crime, i.e. that the restriction on the right of access under second 5(1) (a) applied to the legislation. The report noted that an Garda Síochána were

seeking the advice of the Attorney General on this point.

It may be noted that the 2011 Act limits the circumstances in which retained data may be accessed (section 5) and provides a complaints procedures and review of its operation by a designated judge (sections 10 and 12). However it does not lay down clear and precise rules on the scope and application to a much greater degree than the Directive itself, and in particular there is no duty to inform persons whose data may have been retained of their retention, access, or use whether lawfully or unlawfully. Also while access to the data is limited to the circumstances identified in section 5 the obligation to retain data is not limited, and applies generally to all data, and all service providers falling within the terms of the Act.

The act also does not require a reasoned request, nor a prior review of the request before a disclosure request can be made by the superior officers who can make such requests from the service providers.

Despite the limitation periods when such data can be retained there is no specific restriction on the period of retention requiring it to be based on objective criteria in order to ensure that it is limited to what is strictly necessary. The Act also does not make specific provisions for destruction of the data beyond a particular period, and does not exclude retention of data outside the European Union.

The 2011 Act, may therefore, despite the Dwyer Judgement, be vulnerable to challenge on the basis of EU law In case C-617/10 Alerbrg Fransson the ECJ held that member states must comply with fundamental rights as protected in the EU legal order even when they derogate from rules of EU law.

In this case although the Directive has now been declared invalid it is arguable that member states such as Ireland in enacting and applying national data retention measures continue to "implement" or act within the scope of Union law for the purpose of article 51 (1) of the Charter.

While the Directive has been struck down, the e Privacy Directive 2002 /58/EC remains in force. This directive applies a specific application of the Data Protection Directive to the electronic telecommunications sector, and provides that member states may inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in the directive. Ireland relied on this provision to put in place a data retention regime under part 7 of the Criminal Justice (Terrorist Offences) Act 2005 which was repealed by the 2011 Act It may be argued that at least certain aspects of the data retention regime under the 2011 Act fall outside the scope of union law in light of article 1(3) of the e Privacy Directive which provides that the Directive shall not apply to activities falling outside the scope of the Treaties including activities concerning public security, defence, state security, and the activities of the state in areas of criminal law.

If Ireland is still acting within the scope of Union law so that the Charter is applicable to the 2011 Act, it may be that the 2011 Act would be regarded as being in breach of articles 7 and 8 and 52 (1) of the Charter for many of the same reasons that the ECJ found the Directive to be in breach of Articles 7 and 8. If the ECJ found this to be the case then at a minimum the state would have to disapply the 2011 Act if not repeal it entirely or make significant amendments to it to bring it in line with the requirements of the Charter.

Irish Constitutional Provisions and Protections in relation to Privacy

Even if the Charter did not apply to the 2011 Act its validity would have to be assessed having regard to the provisions of the Constitution and the right to privacy as provided for in Article 40.3 as indicated earlier in the Kennedy Judgement and most recently by Judge Hogan in the case of **Maximilian Schrems v the Data Protection Commissione**r.

In **EMI Records (Ireland) Limited & Others v UPC Communications Ireland Ltd (High Court October 11th 2010 -** Charleton J) in the context of an application for injunctive relief by a number of recording companies against a major internet service provider to prevent the theft of their copyright by third parties illegally downloading it over the internet Charleton J indicated that "privacy in the modern panoptic society must be flexible enough to address new technologies and developments and their privacy implications, while at the same time certain enough as to offer guidance and clarity as a matter of law ".

The Judge found that the right to privacy could never extend to conversations emails letters phone calls or any other communications designed to further a criminal enterprise, stating that "criminals leave the private sphere when they infringe the rights of others or conspire in that respect".

It is still likely that the Irish courts would consider the 2011 Act a serious interference with the constitutional right to privacy but would then carry out a balancing act to see if that right interfered with competing interests such as the investigation of crime or public safety.

In June 2014 Mr Justice Hog**an** in the High Court case of **Maximilian Schrems v Data Protection Commissioner Case, h**eld tha**t:**

"The accessing by State authorities of private communications generated within the home whether this involved the accessing of telephone calls, internet use or private mail also directly engages the inviolability of the dwelling as guaranteed by Article 40.5 of the Constitution. ... Naturally the mere fact that these rights are thus engaged does not necessarily mean that the interception of communications by state authorities is necessarily or always unlawful. Provided appropriate safeguards are in place it would have to be acknowledged that in a modern society electronic surveillance and interception of communications is indispensable to the preservation of state security".

The Judge went on however "the importance of these rights is such nonetheless that the interference with these privacy interests must be in a manner provided for by law and any such interference must be proportionate. This is especially the case in respect of the interception and surveillance of communications within the home".

Mr Schrems was objecting to the failure of the Data Protection Commissioner to investigate the transfer of his personal data held by Facebook Ireland to a server in the United States where it could be uplifted on a mass basis with other data by the United States National Security Agency for analysis without his knowledge under a Safe Harbour Agreement between the EU and the US. This agreement allowed him no access to the US courts in order to enforce the correct supervision and protection of that data. Judge Hogan stated that such "a state of affairs with its gloomy echoes of the mass surveillance programmes conducted in totalitarian states such as the German Democratic Republic ... would be totally at odds with the basic premises and fundamental values of the constitution, respect for human dignity and freedom of the individual".

The Judge referred a question to the European Court of Justice seeking its guidance as to whether the Irish Data Commissioner was precluded from investigating the Safe Harbour Agreement reached between the EU and the United States. The ECJ ruled on the 7th of October 2015 that the agreement was in breach of article 8 of the Charter of Fundamental Rights which provides that

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

Because both Mr Schrems and the Irish Data Protection Commissioner could not gain access and investigate how data was transferred to the United State and processed, and because these tasks could not be conducted in the territorial jurisdiction of the Data Protection regimes of the EU Mr Schrems was precluded from exercising his rights under the Charter and the Safe Harbour agreement was therefore struck down by the ECJ.

The result of the ECJ judgement was a massive scramble by the Commission and the US authorities to reach a new agreement that allowed for appropriate access by EU citizens to enforce their data protection rights in relation to data transferred to US soil. This agreement was reached at the end of January 2016 but could still be tested on the same principles again before the ECJ. It appeared at one stage as if any transfer of data generated within the EU to the US would have been ordered to be stopped unless a new agreement was reached, and unless the Data Protection officers in Europe could certify that US law on data protection met the standards of protection and supervision set by EU jurisprudence and the Charter.l. It is to be noted that recently the US congress has introduced legislation to allow non US citizens to seek review of access to their data before the US courts.

Recent legislative attempts to deal with ECJ jurisprudence and recent case law

The Parliament of the United Kingdom passed an Act on the 17th of July 2014 to deal with the consequences of invalidity made by the Court of Justice in relation to Directive 2006/24 EC. This indicated that the Secretary of state can issue a data retention order if he considers it necessary for the purposes of complying with the UK Investigatory Powers Act 2000 The retention period must not exceed twelve months ,and the Communications Commissioner must review the interception of any data on a half yearly basis, and there must be an independent reviewer of terrorism legislation to review the operation and regulation of investigatory powers , and these reports must be submitted to Parliament for review as well as any regulations made under the Act. The Act was challenged by MPS Tom Watson and David Davis who were supported by the Human Rights organisation Liberty. The High Court in the UK ruled that certain retention obligations under the Act should be disapplied on the basis of inconsistency with the protections under Article 7 and article 8 of the Charter of Fundamental Rights of the European Union in light of the Digital Rights Ireland case.

The High Court held that the powers conferred by the United Kingdom Act were disproportionate in light of articles 7 and 8. In particular the Court objected to the lack of clear rules restricting access and use of retained data to the investigation or prosecution of serious criminal offences, and the fact that the access was not dependent on prior administrative/judicial review.

Mutual Legal Assistance and Cybercrime

The Irish Criminal Justice (Mutual Legal Assistance) Act 2008 allows the authorities in Ireland to apply for evidence from other jurisdictions based on the various conventions and treaties outlined in that legislation.

The Act provides for the exchange of evidence on a cross border basis. Evidence is defined in section 2 as oral evidence or as appropriate any document or thing which could be produced as evidence in criminal proceedings The Act provides for the taking of evidence from a person in a designated state for the purpose of a criminal investigation or proceedings. This is done by means of a letter of request from a judge of any court upon application by the DPP or an accused person.

The request shall include a statement that the evidence is needed in criminal proceedings a description of the conduct concerned and any other information that may assist the designated state in complying with the request. There is an obligation to return the evidence after the proceedings have ended. The Irish Court retains its discretion as to whether to ultimately admit the evidence at trial Section 73 empowers a judge to seek assistance from a designated state in order to obtain evidence. Section 73(8) provides that such evidence (apart from documentary evidence)is admissible without further proof. . As with the other measures there are corresponding provisions in the event that the request comes from a member state seeking to use the evidence in that state.

The Director is a judicial authority nominated by Ireland, as well as the courts, and the Chief State Solicitor. The Director can apply for evidence to be frozen or obtained using the procedures as set out in that legislation. The office of the DPP deals with all outgoing mutual legal assistance requests as requested by An Garda Síochána.

Proving automatically recorded data in the context of mutual legal assistance

Despite the provisions of the Criminal Evidence Act 1992 and the Electronic Commerce Act 2000 difficulties have still arisen in relation to proving documents automatically generated without human intervention The Irish Courts have felt bound by the principles enunciated in DPP v Brian Meehan 2006 3 IR where the court ruled that telephone data was admissible as real evidence where it had been produced during an automated process without any human intervention. No evidence was required from a person as to the input of the data as under section 5 of the 1992 Act The court found however that it was incumbent on the prosecution to call appropriate authoritative evidence to describe the function and operation of the computer The court followed an English case called Cochrane that applied the UK PACE act which had in fact been abolished as being unworkable As such it has been argued that the common law principle should be applied that it must be assumed until proven to the contrary that all machinery is operating normally and effectively at all relevant times.

Another problem that has arisen in the last few years is the need to obtain electronic evidence from service providers abroad i.e. content and non-content information from computer service provides such as Facebook, Google Microsoft and Yahoo, some of whom have their European Headquarters in Ireland.

In a Central Criminal Court case called DPP -v- MB in 2014 evidence was admitted of incriminating statements by the Accused on his Facebook profile in conversation with three separate person on the day following the murder of M B. Arising out of the information obtained from one of

these people Gardaí requested the digital records of four Facebook accounts including that of the Accused from Facebook in the states.

Originally the material had been obtained from Facebook Ireland when the guards served a section 10 Miscellaneous Provisions warrant on Facebook Ireland. The relevant material was emailed to the guards without any covering affidavit or statement. The material was also obtained through mutual legal assistance requests from Facebook US under the terms of the Ireland United Sates Mutual Assistance in Criminal Matters Treaty in 2001. The downloaded records came in the form of PDF documents which were accompanied by a certificate statement made by an employee of Facebook who described herself as a record custodian. Prosecution counsel had advised that there was a difficulty with proving the said records as there was no evidence adduced by the relevant official as to the operation or reliability of the computerised system from which the relevant material was downloaded. Counsel advised that a statement be obtained from the relevant official in line with the Meehan decision describing the operation and reliability of the computer system at all material times Counsel also requested that the relevant official be made available to give evidence in court.

This request was rejected by the service provider However article 8 of the 2001 Treaty provides that the Central Authorities of both countries could from time to time agree changes to the terms of authentication by way of certificate that accompanied the relevant information disc A new form of certificate was agreed in September 2014 between the relevant central Authorities which indicated that the information contained in the records was automatically created by and accurately captured from user generated communications and computer transactional data and was relied upon in the operation of the business of Facebook Inc The Trial Judge accepted this certificate was sufficient evidence of authentication of the computer system and that the prosecution was entitled to rely upon the common law presumption that mechanical devices were in proper working order at the relevant time or times. Another judge in Leitrim in a sex offences case rejected this type of evidence.

The DPP -v MB decision was appealed by the Defence to the court of Appeal and a decision is awaited from that court. A further decision by Judge Birmingham on the 27th of October 2015 in the case of DPP v Marcus Kirwan held that there was no need to prove the effective operation of cctv footage as such systems were well known to all practitioners and was not a novel technology. On the 14th of June 2016 the Court of Appeal held in the case of DPP-v- CC and MF that :-

"Computers vary immensely in their complexity and in the operations they perform. The burden of the evidence to discharge the burden of showing that there has been no improper use of the computer and that it was operating properly will inevitably vary from case to case. I suspect that it will very rarely be necessary to call an expert and that, in the vast majority of cases, it will be possible to discharge the burden by calling a witness who is familiar with the operation of the computer in the sense of knowing what the computer is required to do and who can say that it is doing it properly."

The Judgment implies that proof beyond doubt that a system was not interfered with will not be required in all cases but that some evidence in relation to the operation of a computer system is still required depending on whether the evidence is essential or not.

In the interim lengthy statements are requested from service provider officials in other non US states asking them to state whether to the best of their knowledge their computer systems were

operating normally and accurately at all relevant times. To the best of my knowledge no non us service provider has ever provided such evidence and it may be impossible to provide.

Mutual Legal Assistance in the Light of the Schrems and other EU decisions

The Schemes decision may also have an effect on the mutual legal assistance and cybercrime investigations from an Irish point of view. As the ECJ ruled that the safe harbour agreement was contrary to the right to protection of personal data as provided for in article 8 of the Charter of Fundamental Freedoms there has been more discussion about service providers been forced to ensure that data is available to be accessed in the countries where it is generated.

Already Facebook have indicated that they are building a huge data storage centre in County Meath and another such centre iss operational in Sweden.

In a Belgian Supreme Court Decision called the **Yahoo** case a Belgian prosecutor sought data information from Yahoo in relation to a Belgian criminal investigation. Yahoo, who does not have any head office in Belgium, argued that as the information had been transferred to the United States and a mutual legal assistance request was required. The prosecutor refused, and served a production order on the service provider based on the Belgian Criminal Code which provides:-

"Electronic communications services are defined by the Act of 13 June 2005 on electronic communications as "services normally offered in exchange for payment, which entirely or principally consists of the transfer, including switching and routing processes, of signals via electronic communications networks".

Thus, according to this definition, electronic communications services are services that consist of the transportation of signals (data) over an electronic communications network (eg, broadbandinternet access, telephone lines, cell phone connections).

This is where the first of the two decisions of the Supreme Court comes in. On 18 January 2011, the Belgian Supreme Court decided that "anyone offering a service which consists of allowing its customers to obtain, receive or spread information via an electronic communications network, can be a provider of electronic communications services".

On 4 September 2012 the Supreme Court, in its second decision in the *Yahoo!* case, ruled that the request sent by the Belgian prosecutor was valid after all. According to the Supreme Court, the fact that the Belgian prosecutor sends his request to cooperate on the basis of section 46bis CCP, from Belgian territory to the foreign address of a provider of electronic communications services located abroad, does not make such request invalid under Belgian law.

In the EU judgement C131-12 the **Google Spain v Mario Gonzalez** the right to be forgotten case- the ECJ ruled in 2014 that

"Google Spain is a subsidiary of Google Inc. on Spanish territory and, therefore, an 'establishment' within the meaning of the directive.[The Court rejected Google Inc.'s argument that it was not carrying out its data processing in Spain, holding that the promotion and selling of advertising space by its subsidiary Google Spain was sufficient to constitute processing within the meaning of the Directive. The court held that to have ruled otherwise would have been to undermine the effectiveness of the Directive and the fundamental rights and freedoms of individuals that the Directive seeks to ensure. The Court thus endorsed the Advocate General's view that Google Inc.

and Google Spain should be treated as a single economic unit.

In the United States the Department of Justice has sought a court production order under section 2703 of the United States Stored Communications Act against Microsoft in relation to an email account. Microsoft had in fact built a storage facility in Ireland.- see **Microsoft Corporation v United States of America**

The company argued before the US court of Appeals that the data belonged to the user, and that the DOJ should seek the information requested under mutual legal assistance from its Irish subsidiary. The Irish government along with a number of other interested bodies joined the case as amici curiae and Ireland notified the United States court of an Irish Supreme Court case called Walsh -v National Irish Bank 2013 1 IESC where the court held that the revenue commissioners could seek a production order against an Irish subsidiary of the Bank of Ireland in the Isle of Man where there was no tangible or corporeal differences between the two units.

The US Department of Justice has argued that Microsoft is a US company, and that it can retrieve the requested information with a few clicks of a computer keyboard, and no formal mutual legal assistance request was necessary to Ireland.

Microsoft had engaged Mr Michael McDowell SC to argue that disclosure of data is only legal in this context if authorised by an Irish Judge. Mr McDowell argued that the treaty between the US and Ireland and procedures were designed to apply under precisely these circumstances, and Ireland is obliged to protect data on its soil from foreign law enforcement Echoing privacy activists in the United States Mr McDowell said in his argument that in part this was about Irish sovereignty. . “Ireland's data protection acts “highlights its sovereign interest guarding against foreign law enforcement within its borders by any means other than applicable mutual legal assistance treaties. Any disclosure of data held in Ireland “ is only lawful where such disclosure is required or mandated by reference to Irish law and subject to the jurisdiction and control of the Irish court.”.

On July 14 2016 a three judge panel of the Second Circuit ruled in favour of Microsoft applying the 2010 US Supreme Court decision Morrison v National Australia Bank which held that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States, and that this rule applies in all cases. The Second Circuit found no mention of extraterritorial application in the US Stored Communications Act (SCA) enacted in 1986 before the World Wide web or cloud computing existed, nor in its legislative history

There appears to be heightened interest in this case as it appears to be one of the cases generating a climax to the issue as to whether service providers can be coerced into cooperating with law enforcement agencies in relation to such requests and even with the law enforcement agencies of foreign jurisdictions.

It has been argued that if the Department of Justice in the US eventually succeeds before the US Supreme Court that it will force the EU to push further for the retrieval of information transferred by US European subsidiaries to the states.

The striking down of the safe harbour agreement has serious consequences for the storage and location of data. If a new agreement had not been reached at the end of January in relation to new safeguards between the US and EU then it would have been likely that all EU data protection

officers could have been forced to order that the transfer of all such data should stop. As most of the big US service providers have their corporate headquarters in Ireland this would have meant that Ireland could be the target of a large number of incoming requests for mutual legal assistance from other EU countries for data stored or not stored in this jurisdiction, even if it was transferred to the US, and the effect of the Yahoo and Belgium and the Google cases, and the ability of countries and individuals to seek access to data from where ever the information was generated brings the objectives of the Budapest convention into sharp focus.

What is around the Corner: - The European Investigation Order Directive, The Data Protection Directive and the Date Protection Regulation

Data Protection Directive 2015 (to be transposed into domestic legislation by 2018)

In essence the Directive deals with the processing of data related to criminal investigations and prosecutions. The Regulation deals with the processing of all other data and provide for the harmonised processing of data in the EU.

All data collected by law enforcement authorities must be collected on the basis of the principles set down in the directive, ie collected fairly, for specific explicit and legitimate purposes, to be kept in a form which permits identification of the data subject for no longer than is necessary, that it is kept secure from illegal access, and against accidental loss.

Article 5 of the Directive states that member states should set time limits for the erasure of personal data, or for a periodic review. How this might affect data collected during the course of a criminal investigation or criminal proceedings, where it may be necessary to retain same for indefinite periods for the purposes of appeal or for the purpose of review of unjustified prosecution or investigation is not yet known

Member states are supposed to provide distinctions in processing data between data relating to defendants, victims, convicted criminals etc. How again this is to apply is not yet known

Article 12 sets out the obligations of the data controller in relation to data assess requests, and appears to allow for access requests to be refused where they are excessive. Again it is not clearly defined what excessive means, but it appears that the burden of proving that such a request is excessive lies on the controller.

The controller can restrict the right of access to the data subject as long as it is proportionate, ie if to do otherwise would undermine ongoing investigations or prosecutions or to protect public or national security.

Article 14 obliges the controller to inform the subject if their data has been

transferred to other agencies, and for what purposes, and in particular if that data has been handed over to third countries outside the EU, presumably after the relevant investigation is completed

The obligations on the data controller to ensure that processors maintain data within the directive's parameters is also set out. How disclosure to defence lawyers is to be dealt with, and whether they are data controllers within their own right has still to be defined in legislation.

Article 25 obliges the data controller to maintain logs of how and when data is processed, transferred and to whom, and when it is erased.

Under chapter five of the Directive if data is being transferred to third countries by way of mutual legal assistance,(i.e transfer of proceedings or extradition or mutual legal assistance)) the transferring country must confirm with the EU commission that such third country provides equivalent/ adequate data protection as that of the EU. If the commission is unable to provide such confirmation the obligation to ensure equivalence rests on the body transferring the data

Article 47 empowers the relevant data protection commissioner to direct the banning of processing of data by the relevant controller if there is a breach of the Directive.

European Investigation Order

Under the Lisbon Treaty of 2009 Ireland and the United Kingdom negotiated an "opt-out" protocol which extends to the field of criminal justice co-operation. The initiative for a directive on a European Investigative Order was undertaken by a group of member states which seek to replace the current system of mutual Legal Assistance in the EU with a single regime for obtaining evidence located in another member state. It is intended that the Directive may be used for obtaining evidence in criminal matters and covers all investigative measures.

The Directive concerns the whole range of criminal proceedings from less serious offences to organised crime like trafficking in human beings and terrorism. No de minimis rule can be applied by any country that opts into the Directive.

At present it is believed that approximately 90% of incoming requests relate to information held by service providers such as bank, telephone companies etc. At present the Central Authority engages the services of An Garda Síochána and the Chief State Solicitor's Office acting on behalf of the Minister for Justice (the Central Authority under the 2008 mutual assistance act) and the provisions of section 75 of the Criminal Justice (Mutual Assistance) Act 2008 to obtain court production orders for the bulk of incoming requests. Section 63 of the same act is utilised in a small number of cases when oral evidence is required from witnesses summonsed to court for the production of certain types of documents.

The Directive in article 2 provides that EIOs issued by E\U states shall be issued by issuing authorities and executed in EU states by executing authorities. The Directive specifies that the

issuing and executing authorities may be a judge court an investigative magistrate or a public prosecutor, or any competent authority as defined by the issuing state.

Judge Denham in the Supreme Court case **of Jason Brady -v- Judge Gerard Haughton and others 29th of July 200**5 set out some principles for the operation of mutual legal assistance as it applied in an Irish context. She noted that the role of an Irish court under the mla legislation at the time (The 1994 Criminal Justice Act) was purely administrative in nature. Judge Denham however went on to note that "certain problems may arise in giving mutual assistance in criminal matters between countries with differing legal systems. Indeed the fact that most European states have a civil law system is reflected in the convention and this may cause problems in the future in the steps required to implement the law"

The Judge noted that the Irish mla legislation at present allowed for review and appeal in Ireland and noted that the assistance provided must relate only to the specific request and that if any of the information requested was intended to be used for a criminal trial, and should there be an issue of evidence at trial at a later stage then "further steps would be required".

Article 13 of the Directive has indicated that parties that seek to contest the substantive reasons for issuing an EIO can only mount a legal challenge in the issuing state. Under Article 8 all EIOs must be mutually recognised by the executing state, and such an order can only be challenged through the use of grounds for refusal set out in article 10 i.e. if the offence being investigated is not one of the offences set out which are basically the same offences as set out in the EAW directive.

The executing authority will still use a production order/search warrant mechanism where appropriate if the state opts into the EIO directive. (be it under a particular criminal statute or if possible under a catch-all EIO statute. If the offence is one of the 32 EAW offences, the executing authority would be obliged to execute a "search and seizure " order even if the measure cannot be used domestically. Article nine provides that where there is no corresponding investigative provisions in domestic law that can be used in respect of the conduct giving rise to the EIO that the executing authority would be obliged to use some other investigative measure that is available under domestic law. This would be done at the discretion of the Executing Authority provided it can achieve the same result as intended by the EIO.

Article 18 refers to the protection of personal data. The executing authority will have to set up procedures and guidelines for the protection of personal received by it and presumably would come under the supervision and scrutiny of the Data Protection Office.

The EIO also deals with such issues as the transfer of prisoners and also under article 23 specifies that an EIO may issue for wide ranging banking information. Article 27 provides for monitoring of banking operations and covert operations.

Conclusion

The area of cyber-crime law enforcement and co-operation, with the requisite obligation to respect the rights to privacy of individuals is developing as quickly as the technological tools and processes used to effect criminal activity.

The tools available to various law enforcement agents do not appear to be regarded highly by them and are often considered to be "cumbersome" and "antiquated" considering the vast paced nature of technological change. Law enforcement agencies have pushed for ever greater access to data

systems and quicker response times in relation to same. The problem with such a movement is that there appears to have been a popular backlash against "mass surveillance and data collection" by law enforcement agents particularly after the Snowden revelations in 2013.

Ireland in particular has been the focus of this backlash recently because of the Digital rights and Schrems cases, and because of the fact that many global service providers such as Microsoft, Google and Facebook have their European Headquarters in our country.

Despite the JC decision it may be that in the area of essential evidence relating to cybercrime investigations- access to data- that the tide may be turning very quickly against unjustified intrusion into personal data by law enforcement agencies ,and that onerous obligations for court and data protection supervision, as well as a high threshold of suspicion and evidence will be required before such intrusion by LEAs will be tolerated by the courts either at an Irish or EU level in the future. Developing individual rights law in this area would appear to be geared against mass retention of data, towards protection of the privacy of the individual, and even towards the notification of individuals by either the service provider or the investigator of an investigation into their data.

The ECJ held in late 2015 in C201-14 Bara when asked to rule on the legitimacy of the Romanian government's laws allowing for citizens data to be shared by the government between institutions without the knowledge of the person whose data that.

"articles 10 11 and 13 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as precluding national measures such as those at issue in the main proceedings which allow a public administrative body of a member state to transfer personal data to another public administrative body and their subsequent processing without **the data subjects having been informed of that transfer or processing.**

In 2014 the New York Times reported that many service providers were already notifying individual users of investigations into their data despite the requests for confidentiality in the court production orders. Some EU authorities appear to notify suspect of enquiries in relation to their data after a defined period even if investigations have not concluded.

At the moment requests for data from EU states and outside are court supervised under the mla system and can be reviewed even if a wide margin of appreciation is given to the integrity of the requests of issuing states. If the EIO is introduced in Ireland, considering the appetite for electronic evidence from major service providers, and the fact that many service providers will locate most of their data storage in Ireland, this jurisdiction will be flooded with requests from states for production orders. Irish courts will be obliged to give effect to the EIOs and will have very limited and restricted power to refuse execution while at the same time being obliged to provide a high degree of protection to data stored in the country under the 2016 Data Protection directive. Both directives will be supervised by the ECJ which will have precedence domestic courts under Article 28 in this area.

Service providers also habitually argue the jurisdictional issue about data storage and many US subsidiaries argue that the requested data is not stored in this jurisdiction but stored in the cloud, or transferred back to the US where issues surrounding proximate cause and the right to freedom of expression limit certain requests in harassment and incitement to hatred cases and can take months to process anyway. The ECJ does not appear to buy this argument any more, and appears to focus

more on the rights of individuals to the data they generate and to the efficacy of the services provided by the ISPs. The ISPs as are shown by the Microsoft case, and the recent legal battle in the United States between the FBI and Apple appear intent in fighting any domestic non MLA based requests for content information to ensure that the mutual legal assistance process is maintained at all costs. Whether the same protections are provided in relation to requests under the EIO is still to be seen. Some commentators have talked about a "balkanization of data storage".

We live in interesting times.

BIBLIOGRAPHY

1. **The Exclusionary Rule and Search Warrants – Insight- Internal DPP case management**
2. **Electronic Evidence Third Edition- Chapter 14 (Ireland) Ruth Cannon and Katie Dawson**
3. **Electronic Evidence Presentation DPP's Office – Ray Briscoe- 18th November 2015**
4. **Proving Electronic Records- Presentation DPP's Office- Michael Brady 18th November 2015**
5. **Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the EU- Eurojust 10-11 December 2015 (contributed by Tricia Harkin)**
6. **LRC Issues Paper on Cyber-Crime – cyberbullying (LRC IP 6-2014 and various papers prepared by DPP officers in relation to same same (Denis Butler and Deirdre Manninger)**
7. **Transcript of Graham Dwyer Judgment by Judge Hunt 25/2/2015**
8. **"In Memoriam Amore"- Revenge, Sex, and Cyber space- Pauline Walley SC**
9. **Data Protection – Safe Harbour What Next? Arthur Cox Group Briefing October 2015**
10. **ERA- International Data Transfers After the Invalidation of the Safe harbour Decision Brussels 26/1/2016**
11. **Schrems Case- Background & Consequences – An Overview- Noel Travers SC – ICEL Seminar 28/1/2016**
12. **ERA Conference Papers " Countering the Illegal Use of Internet" Stockholm 16th and 17th April 2015 (Contributed by Denis Butler)**
13. **Eurojust- Strategic Seminar "Towards Cooperation in Freezing and Confiscation of the Proceeds of Crime 11-12 December 2014**
14. **European Centre for Monitoring Drugs and Drugs Addiction Report January 2016**
15. **TJ McIntyre judicial oversight of Surveillance: the Case of Ireland in Comparative Perspective.**