Cybercrime: Towards a Research Agenda

TJ McIntyre¹

This is a post-print of a chapter published in Deirdre Healy, Claire Hamilton, Yvonne Daly, Michelle Butler (eds.), *Routledge Handbook of Irish Criminology* (London: Routledge, 2015)

Abstract

This chapter examines cybercrime from an Irish perspective, providing an overview of the domestic situation against the background of the international legal framework. It addresses the prevalence of cybercrime in Ireland and the policing response, looking in particular at resource and management issues within the Garda Síochána. It then outlines the legislation criminalising cybercrime, assessing whether that legislation meets the requirements of European Union law and the Council of Europe Convention on Cybercrime. It concludes by describing the growth of mandatory reporting in this area and the effect which this may have on research into cybercrime.

Introduction

The study of cybercrime in the Republic of Ireland has generally been outward rather than inward looking. There is a growing literature *from* the Republic of Ireland yet there has been relatively little written on cybercrime *in* the Republic. Research such as that of Kirwan and Power (2011, 2013), Conway (2006) and Taylor and Quayle (2008) has for the most part taken a broad international perspective and there has been less attention to topics such as the ways in which Irish law addresses cybercrime, its prevalence, or the manner in which the criminal justice system has responded – though with some exceptions such as the work of Clark and Hyland (2007), O'Donnell and Milner (2007) and Kelleher and Murray (2007).

There are several reasons for this. In some cases it reflects the technical orientation of the research, as in the UCD Centre for Cybersecurity & Cybercrime Investigation which focuses on areas such as forensic analysis. In other cases, the authors explicitly or implicitly treat the issues presented by particular aspects of cybercrime – such as child abuse images – as largely homogenous across different countries (see e.g. Taylor and Quayle, 2003). Throughout the literature, there has been an influential view that cybercrime is an inherently international phenomenon so that equally its regulation and study should presumptively take an international approach (Prins, 2006).

In light of these factors one might ask: why take a specifically Irish perspective? The answer – as with other aspects of internet governance – is that there are important features at the domestic level which otherwise risk being overlooked. A business friendly (and low tax) environment has led to a cluster of internet giants such as Google, Facebook, Microsoft and Twitter setting up regional headquarters in Dublin. Irish law and practice is particularly significant for the way in which it might regulate those firms and their users. Despite this, the Republic of Ireland is an outlier in having failed to update its cybercrime laws – the most important law in this area dates back to 1991 and

¹ Lecturer in Law, UCD Sutherland School of Law; chair of Digital Rights Ireland.

is in urgent need of reform (McIntyre, 2005). Similarly, the Garda response to cybercrime has gone largely unexamined despite significant resource and management problems which have resulted in delays of several years in examining seized computers (Garda Síochána Inspectorate, 2014, pt. 6).

This chapter addresses this gap in the literature by discussing current issues which are specific to the Republic of Ireland against a wider international context. The aim is to provide an introduction to the legal and regulatory framework around cybercrime, highlighting the work which has already been done as well as identifying topics which merit further research. The focus is on the substantive law and the manner in which it has been enforced – procedural issues (such as garda powers to compel decryption of encrypted files²) are not considered.

The geographic scope of the chapter might call for a few words. Why focus on the Republic of Ireland when this Handbook generally takes an all-island perspective? While the constraints imposed by the word limit are a factor, the main consideration is that the substantive law in Northern Ireland largely reflects that of England and Wales and the wider United Kingdom.³ Because of this, Northern Ireland is already well served by an extensive literature on cybercrime in the United Kingdom generally (see e.g. Edwards et al., 2010). That said, there are issues relating to the policing of cybercrime in Northern Ireland which call for more examination and the Policing Board has recently commissioned research on the prevalence of cybercrime which may provide the starting point for further work (Northern Ireland Policing Board, 2014).

Defining “cybercrime”

What do we mean by “cybercrime”? Is it a new type of crime which requires us to develop new concepts for understanding it or new laws to control it? There is a well-known and ongoing debate between those such as Grabosky (2001) who see computer crimes as largely a case of “old wine in new bottles” and those who with Yar (2005) see the unique features of the online environment as giving rise to “a new and distinctive form of criminal activity”. In some ways, however, the difference between the two sides may be more apparent than real – even those who argue against cybercrime as a new form of crime generally accept a pragmatic need for new legislation to address the particular challenges of scale, jurisdiction and evidence which it presents (Brenner, 2001).

This debate as to whether cybercrime is a distinct type of crime is in part an issue of terminology, as the term tends to be applied indiscriminately to any crime involving the use of computers. In response, Wall has developed an influential classification which identifies three generations of cybercrime (2007a, 2007b). The first generation is made up of *traditional or ordinary crimes committed using computers* – for example, where email is used to coordinate a kidnapping. The second generation consists of *hybrid crimes* – traditional crimes which are given new reach, scope or impact due to

² See e.g. sections 48 and 52 of the Criminal Justice (Theft and Fraud Offences) Act 2001.

³ Although Northern Ireland is a separate jurisdiction with devolved powers in relation to policing and criminal justice, those powers only came into effect in April 2010 with the adoption of the Northern Ireland Act 1998 (Devolution of Policing and Justice Functions) Order 2010. Most laws relating to cybercrime were adopted in Westminster prior to that date and the law in Northern Ireland has yet to diverge significantly.

the Internet. Child abuse images exemplify these crimes – while they predated the internet their dissemination has increased exponentially online. The third generation he terms *true cybercrimes* – those which could not exist without the Internet. Examples include denial of service attacks and the distribution of malware. A common feature of most true cybercrimes is that they feature technology as a *target* of crime and not merely an *instrument* of crime (Casey, 2011, chap. 2). Applying this classification, this chapter will consider those issues presented by Wall's second and third generations of cybercrime.

Extent of cybercrime

It is exceptionally difficult to put a figure on the prevalence or cost of cybercrime. The international experience has been that the available statistics are generally fragmentary and inconsistent in the methodologies used and the Republic of Ireland is no exception (Galetsas, 2007; Anderson et al., 2012; McGuire and Dowling, 2013).

At the level of the individual user, the best available sources are the Eurobarometer series of cyber security reports. These are based on surveys of the general population throughout Europe and ask to what extent the respondents have been the victims of various types of cybercrimes. The most recent, carried out in 2014, places Ireland overall somewhat above the EU average for the extent of cybercrime (TNS Opinion & Social, 2015). For example: 40% of those surveyed reported receiving phishing attacks ('emails or phone calls fraudulently asking for access to your computer, logins, etc.') compared to an EU average of 31%. 16% reported their social media or email account being hacked (EU average 12%). 9% reported being the victim of identity theft online (EU average 7%). 7% reported being the victim of ransomware ('being asked for a payment in return for getting back control of your device') against an EU average of 8%.

As regards businesses, the most up to date sources of information are surveys carried out by security vendors who have an interest in talking up the scale of the threat (Deloitte, 2013; PwC, 2014). Consequently, while the surveys contain useful impressionistic information it is difficult to place much reliance on their wider findings. For example, one PwC survey which identified cybercrime in Ireland as doubling between 2011 and 2014 was based on a definition which equated infection by a virus and illegal downloading of music with much more serious offences (PwC, 2014, p. 14). Unfortunately, a more sophisticated survey by UCD and the Information Systems Security Association (ISSA) ran only twice – in 2006 and 2008 – before it was discontinued (O'Connor and Gladyshev, 2006; O'Connor, 2008). Nevertheless, that survey is still valuable for establishing a baseline indicating a high level of threat for Irish organisations – in the 2008 survey 25% of respondents reported suffering at least one external intrusion in 2007 while 32% experienced external intrusions within the previous five years.

The official sources do not take us much further (see chapter xxx for a discussion of the difficulties with official crime sources). Because Irish law generally conceptualises cybercrimes as mere variants of more traditional crimes, the Irish Crime Classification System (ICCS) recognises only one distinct cybercrime – the offence of unauthorised access to data (Central Statistics Office, 2008, p. 14). The most recent Garda recorded crime statistics show this as increasing from seven recorded offences in 2008 to 35 in

2012 (Central Statistics Office, 2014, p. 85). Other cybercrimes are subsumed into the more general criminal damage or dishonesty offences. For example, a prosecution of two students for defacing Fine Gael's website shortly before the 2011 general election was charged as criminal damage and therefore would not be apparent from the statistics (Stack, 2013). A further complication is that the recorded crime statistics do not reflect reports made to other state bodies with investigation and prosecution functions – particularly the Data Protection Commissioner – and there is no statistical data available in relation to these.

There is slightly more clarity in the case of child abuse image offences. Although these statistics are not divided between online and offline crimes, in practice almost all such offences involve the internet and we can identify a growth in recorded offences from 46 in 2008 to 313 in 2012 (Central Statistics Office, 2014, p. 17). In addition, this area was the subject of extensive empirical work by O'Donnell and Milner who have provided detailed figures for investigations and prosecutions over the period from 2000 to 2004 inclusive, including the number and nature of the images involved, profiles of the offenders and analysis of sentencing (O'Donnell and Milner, 2007, chap. 4). They found, for example, that the number of suspects over that period spiked from 6 in 2000 to 104 in 2002 following information received from a United States investigation into those purchasing access to child abuse images. Of the cases examined by O'Donnell and Milner the large majority (79%) related to simple possession; 8% involved distribution or production; 4% involved child trafficking for sexual exploitation and 2% involved allowing a child to be used for pornography.⁴

Cybercrime figures are generally skewed by under-reporting, whether to avoid publicity, because incidents are perceived as too trivial to report, or for other reasons. Gardaí recognise that businesses prefer to avoid reporting cybercrime and have encouraged informal meetings with victims for intelligence gathering rather than prosecution purposes (Smith, 2005). The 2006 and 2008 ISSA/UCD surveys confirmed that Irish organisations generally do not involve law enforcement – for example, where internal personnel were involved, just 18% of organisations reported the matter to police, with the majority letting the matter rest following the dismissal or resignation of the employee (O'Connor and Gladyshev, 2006, p. 26). It is therefore probable that the recorded crime statistics significantly understate the extent of offences.

There are, however, recent developments which may lead to greater reporting of cybercrime and indirectly to more reliable statistics. As we shall see later in this chapter, legislation in 2011 introduced mandatory reporting of certain types of cybercrime (broadly speaking, data breaches in the telecommunications sector, criminal damage to data and crimes of dishonesty). Failure to report is itself a crime. As organisations become more aware of this responsibility it is likely that the number of crimes recorded will increase significantly.

Policing of cybercrime

Garda Síochána

⁴ Numbers do not sum to 100% as some respondents did not specify the offence involved.

The primary responsibility for investigating cybercrime in the Republic of Ireland lies with the Computer Crimes Investigation Unit (CCIU) in the Garda Bureau of Fraud Investigation (GBFI). Cases involving child abuse images are the responsibility of the Paedophile Investigation Unit (PIU) in the National Bureau of Criminal Investigation (Garda Síochána Inspectorate, 2014, pt. 10). Both units have a mixed role, carrying out some complex investigations themselves and also providing support to other investigations carried out in local districts.

This split structure has been criticised and in 2005 Eugene Gallagher, then deputy director of the GBFI, described it as leading to investigations which were “reactive and fragmented”. Instead, Gallagher recommended that the Garda Síochána should proceed with internal proposals for a dedicated National Cyber-Crime Unit, following the UK model (Gallagher, 2005). To date, however, there has been no structural reform.

These units have had significant resource problems. Jewkes and Andrews (2005) have highlighted the demands presented by investigation of child abuse images and in an Irish context these have been further exacerbated by limited funding. In 2014, the Garda Inspectorate reported that the PIU had only one computer set up to receive and download evidence, which could be tied up for days at a time dealing with a single case (Garda Síochána Inspectorate, 2014, pt. 10). That report also noted that the PIU used a paper system for managing investigations, raising the possibility that two investigators could be looking at the same suspect unbeknownst to each other.

The position in the CCIU has been equally problematic. One of the main tasks of the CCIU is the forensic analysis of seized computers and mobile phones. This work has, however, grown exponentially as the investigation of almost all serious crimes now involves the seizure and analysis of multiple computing devices (PCs, laptops and a range of smartphones and tablets). The result has been a two to four year delay in analysing these devices, jeopardising a number of prosecutions (Garda Síochána Inspectorate, 2014, pt. 10; Mooney, 2014). As of 2013, there were 25 gardaí allocated to the CCIU and – following media attention – a further eight were promised in 2014 (Rogers, 2014). It remains to be seen whether this increase will be sufficient to eliminate the backlog.

Apart from resource problems the Garda Inspectorate has also highlighted difficulties in the way in which the CCIU and PIU interact with local investigators (Garda Síochána Inspectorate, 2014, pt. 6). For example, the CCIU has reported that it is struggling with unnecessary examinations of devices and would prefer that investigating gardaí carry out preliminary checks at the point of search or seizure to assess whether a device is likely to contain any evidence. The Inspectorate has suggested that this approach should be developed by following the practice in some other jurisdictions of including computer analysts on searches or providing gardaí with triage tools which would automate the process of carrying out initial inspections.

This suggestion is, however, somewhat unrealistic so long as local policing itself also suffers from limited access to technology and training. In 2012, it emerged that two in every five Garda stations were not networked and did not have access to the PULSE database or internal email while the 2014 Garda Inspectorate report found that even in networked stations not all gardaí had access to external email (Garda Síochána Inspectorate, 2014, pt. 7; Reilly, 2012). It is not surprising, therefore, that there has

been a practice among gardaí of using personal devices to get work done – which, quite apart from the security concerns it presents, suggests that in many cases local stations are not adequately equipped to respond to even basic types of cybercrime (Stack and Carty, 2013).

Data Protection Commissioner

The Data Protection Commissioner (DPC) is adopting an increasingly important role in policing cybercrime. While the DPC has always had a prosecution function for certain data protection breaches, until recently the DPC – in common with most Irish regulators – showed a strong preference for soft enforcement measures and the use of civil rather than criminal procedures. This began to change from 2007 onwards when there was a policy change to move towards prosecutions for spam – unsolicited marketing text messages, telephone calls and emails (Data Protection Commissioner, 2008). More recently, the DPC has brought prosecutions in a number of serious cases involving private investigators selling on personal information wrongfully obtained from Department of Social Protection, Garda and Health Service Executive databases (McGuire, 2014; Edwards, 2014; Tuite and Kennedy, 2012). Although resource intensive, the trend towards more prosecutions seems set to continue following a government decision in 2014 to prioritise data protection by doubling funding for the DPC (McMahon, 2014).

Private policing

The focus in this chapter is on the role of the state in regulating the internet through the use of the criminal law. But this must be seen against a context of internet governance where the state plays only a limited part (Riley, 2013). Wall, for example, has highlighted the range of policing functions carried out by internet service providers, social networking sites, online marketplaces, payment providers and users themselves and has argued that the public police must develop a new understanding of their role as one node in the wider network of internet security (Wall, 2007b). Looking at the same phenomenon, Yar (2010) has identified private policing online as posing particular threats to accountability (as private actors take on law enforcement roles without being answerable to democratic institutions) and equity (as internet security may become a commodity to be purchased rather than a public good). Consequently any analysis of internet policing would not be complete without some mention of the ways in which law enforcement functions have been taken on by private entities.

Hotline.ie

The best known Irish instance of private policing is the system operated by the Internet Service Providers' Association of Ireland (ISPAI) which establishes a code of practice for internet service providers (ISPs), a public website for reporting illegal content (Hotline.ie) and general public awareness programmes around staying safe online (Internet Service Providers Association of Ireland, 2014). This was established following the 1998 Department of Justice *Report on Illegal and Harmful Use of the Internet* which recommended the establishment of a self-regulatory system and has remained essentially unchanged since (Working Group on the Illegal and Harmful Use of the Internet, 1998). The system is funded in part by industry and in part by European Union Safer Internet programmes. It works closely with gardaí and the Department of

Justice and Equality, though it has no legislative basis (Clark and Hyland, 2007). It requires Irish ISPs to remove content hosted by them which the Hotline service deems to be “probably illegal” – that is, in violation of the criminal law – but in practice focuses on child abuse images and incitement to hatred.

Similar systems in other jurisdictions have been criticised for the way in which they involve private bodies making assessments of legality (Laidlaw, 2012). However the Hotline.ie system has mostly escaped such criticism, due largely to the pragmatic way in which the ISPAI has resisted any expansion of its remit – because it is limited to material hosted by ISPAI members and does not deal with site blocking, it does not attempt to take on a wider censorship role for Irish internet users. Indeed, it has been argued that self-regulatory systems of this sort can promote freedom of expression by establishing consistent decision making and enabling ISPs to resist arbitrary demands for censorship (Edwards, 2009).

Internet blocking

Internet blocking is one of the most controversial examples of private policing internationally and the Irish experience is set to follow suit (Demeyer et al., 2012). From 2008 onwards, Irish mobile operators have deployed blocking systems preventing access to websites alleged to host child abuse images (GSMA, 2008; GSMA Mobile Alliance Against Child Sexual Abuse Content, 2008; van Turnhout, 2013). In 2014, following pressure from the Garda Síochána and the Department of Justice, UPC became the first fixed line broadband provider to do likewise (Duncan, 2014; UPC, 2014). These blocking systems are, however, of questionable legality (Akdeniz, 2011; McIntyre, 2013). Unlike the better known case of file sharing websites, where ISPs block access on foot of court orders, this type of blocking takes place without any prior notice, judicial involvement or legislative basis.⁵

The Garda/UPC blocking system is particularly problematic. In that system UPC have agreed to block sites designated by the Garda Síochána as containing child abuse images. The blocking appears to take place at the domain level rather than the page or image level (e.g. blocking *all* access to example.com, not merely the particular images on example.com/users/johndoe/illegalmaterial.html), making it likely that there will be over blocking of innocent content. The system is essentially the same as a previous Dutch model – which was abandoned in 2008 following a government study finding that it was ineffective and also contrary to the European Convention on Human Rights in lacking a statutory basis (Stol et al., 2009).

For the same reason, this system would not seem to meet the requirements of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography. Article 25 of that Directive permits the use of blocking by member states, but subject to the requirement that any blocking measures:

must be set by transparent procedures and provide adequate safeguards, in particular to ensure that the restriction is limited to what is necessary and proportionate, and that users are informed of the reason for the restriction. Those safeguards shall also include the possibility of judicial redress.

⁵ Compare *EMI v. UPC* [2013] IEHC 274 in which the High Court ordered a number of ISPs to block access to The Pirate Bay – but only on the basis of a statutory provision allowing this to be done.

The structural over blocking in the Garda/UPC system and lack of any legal basis or judicial redress make it likely that it would fail this requirement unless it can be classed as merely a “voluntary industry action” so as to fall outside the scope of the Directive.⁶ In a 2013 report, Senator Jillian van Turnhout – an advocate of blocking – noted these issues and recommended that a specific legal basis should be put in place for any Irish blocking system (van Turnhout, 2013). It is unfortunate that her points and the wider international experience appear to have been ignored.

Legislative framework

Irish law does not recognise a distinct concept of cybercrime and does not have any statute dedicated to computer or internet crime. Although specific legislation has been promised many times since the Republic of Ireland signed the Council of Europe Convention on Cybercrime⁷ in 2002, successive Ministers for Justice have failed to deliver. As a result, the Republic is an outlier internationally – all other EU member states bar Greece, Poland and Sweden have ratified the Convention while in the wider common law world both Australia and the United States have ratified the Convention and Canada is set to do so shortly (Grigsby, 2014).

This failure to legislate is surprising given the central role of information technology in the Irish economy and is doubly so given that it has also put the Republic of Ireland in breach of its EU obligations. While the Cybercrime Convention is not binding on the Republic until it is ratified, key parts of the Convention are reflected in two European instruments – the 2005 Framework Decision on attacks against information systems⁸ (which should have been transposed by March 2007) and the 2013 Directive on attacks against information systems (which should be transposed by September 2015).⁹ At the time of writing, a bill to transpose the 2013 Directive and enable ratification of the Convention is expected in late 2015 – making it almost certain the state will fail to meet the September 2015 deadline also (Kehoe, 2015).

The lack of standalone legislation means that cybercrimes are for the most part conceptualised as variants of more traditional offences, with varying degrees of success. A full account of these crimes is beyond the scope of this chapter, and in any event is unnecessary given that there have been a number of pieces written on the individual offences (Clark, 1994; Clark and Hyland, 2007; Kelleher and Murray, 2007, pt. 7–8; Koops and Robinson, 2011; McIntyre, 2008, 2005; Murray, 2001; Ryan et al., 2013; Ryan and Harbison, 2010). However it will be useful to survey the main offences to highlight the most important issues which they present. We will do so using the four part classification of the Cybercrime Convention before going on to consider other

⁶ Recital 47 provides an ambiguous carve out from Article 25: “The measures undertaken by Member States in accordance with this Directive in order to remove or, where appropriate, block websites containing child pornography could be based on various types of public action, such as legislative, non-legislative, judicial or other. In that context, this Directive is without prejudice to voluntary action taken by the Internet industry to prevent the misuse of its services or to any support for such action by Member States.”

⁷ CETS No. 185.

⁸ Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

⁹ Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

cybercrimes falling outside the scope of the Convention (the following sections are based in part on McIntyre, 2008).

Offences against the confidentiality, integrity and availability of computer data and systems

The first category of offences required by the Cybercrime Convention are “the core of computer-related offences... representing the basic threats... to which electronic data processing and communicating systems are exposed” (Council of Europe, 2001, para. 35). There are five types of offences under this heading: illegal access to a computer system, illegal interception of data, interference with data, system interference and misuse of devices.

In this category the Republic of Ireland has few matching offences. Most are contained in the Criminal Damage Act 1991 which, despite predating the modern Internet, is still the most important law in this area. That act was not drafted with computers in mind but was initially intended to address damage to tangible, physical property. The provisions regarding cybercrime were shoehorned in at a late stage in the drafting in a way which has caused difficulties since (McIntyre, 2005). For example, the terms ‘operate’ and ‘computer’ are not defined in the 1991 Act – leading Murray to argue that it may be unconstitutionally vague (Murray, 1995). Similarly, offences under the 1991 Act are not defined in terms of whether an individual is authorised or permitted to do something but rather depend on whether the individual acts ‘without lawful excuse’, a term which is only partially defined in section 6. This leaves it unclear whether an offence is committed if, for example, a website user does not abide by the site terms of use (Licken, 1998).

Illegal access to a computer system

Illegal access under article 2 of the Convention is closely matched by the offence of unauthorised access under section 5 of the Criminal Damage Act 1991 which provides:

A person who without lawful excuse operates a computer (a) within the State with intent to access any data kept either within or outside the State, or (b) outside the State with intent to access any data kept within the State, shall, whether or not he accesses any data, be guilty of an offence...

This section has extraterritorial effect and covers those based abroad who target Irish computers as well as purely domestic attackers. It is an attempt offence in that it criminalises those who operate a computer with intent to access any data, whether or not they succeed in doing so. It is, however, problematic.

We have already seen that the terms ‘operate’ and ‘computer’ are not defined in the Act. Similarly, it is unclear what is meant by ‘lawful excuse’ in this context. Does it refer to entitlement to operate the computer, to access the data, or to both? The partial definition of ‘lawful excuse’ in section 6 asks whether there is consent to “*accessing of the data concerned*” – not merely whether *operation of the computer* is with consent. This appears to say that a person is guilty of an offence if they use their own computer to view a file which, as a matter of civil law, they are not entitled to view. If so, this might mean that a journalist would be guilty of unauthorised access by opening a file emailed to them by a whistle-blower (Kelleher and Murray, 2007, p. 709).

A practical issue is that the offence is summary only and carries a maximum term of imprisonment of three months. As a result, many investigative powers (which generally apply only to serious offences) will not be available and any proceedings must be commenced within six months from the date of the offence (Kelleher and Murray, 2007, p. 712). It will be difficult for prosecutors to finalise charges in this complex area in that time, particularly given the resource constraints outlined in this chapter.

Illegal interception of data

Irish law does not have a direct counterpart to the offence of illegal interception of data under article 3 of the Convention. The closest offence is interception of telecommunications contrary to section 98 of the Postal Telecommunications Services Act 1983 (Hall, 1993). This prohibits the interception or disclosure of telecommunications messages being transmitted by ‘authorised undertakings’, meaning those public telecoms operators who are required to be authorised by ComReg (including, for example, all landline and mobile operators).

This is much narrower than the Convention offence and will not apply to communications being transmitted by an entity which is not an ‘authorised undertaking’. For example, a webmail provider such as Gmail would not be covered, nor a university in providing internet access to staff and students, nor a social networking site in respect of private messages between its members. In those situations, if a person were to read users’ messages no offence would be committed under section 98 – leaving many communications unprotected by the law (Kelleher, 2006, p. 454).

The reference in section 98 to messages ‘being transmitted’ also presents problems. This appears to suggest that only messages in transit are covered: stored messages, such as voicemail messages which have been listened to but left on the server, may not be protected by the section.¹⁰ If so, this presents some difficult questions of interpretation. For example, is an email ‘being transmitted’ until such time as it is read by the recipient (Kelleher, 2006, pp. 454–458)? To date there appears to have been only one prosecution under section 98 – a District Court case involving a civil servant who was found guilty of listening to voicemails left on the mobile phone of her former supervisor (Tuite, 2013). That case did not, however, address the ‘being transmitted’ issue, leaving us without any guidance on this point.

Data interference

The article 4 Convention offence of interference with data is roughly matched by criminal damage to data under section 2 of the 1991 Act. Section 2 is not specific to computers but is a general offence committed by a person who without lawful excuse damages ‘any property’ either intentionally or recklessly. It is extended to computers by the very wide definition of ‘property’ in section 1 to include data¹¹ as well as tangible property. ‘Damage’ to data is then defined to include any ‘addition, alteration, corruption, erasure or movement’ of that data.

¹⁰ Compare *Edmonson, Weatherup, Brooks, Coulson & Kuttner v. R* [2013] EWCA Crim 1026, holding that “phone hacking” of stored voicemails was within the scope of the (differently worded) UK Regulation of Investigatory Powers Act 2000.

¹¹ Defined as “information in a form in which it can be accessed by means of a computer”.

This is an expansive offence: unlike criminal damage to tangible property (which requires some adverse effect) criminal damage to data will include any modification of any information stored on a computer whether or not it causes any interference with the system. Because of this it can potentially be used against a wide range of conduct. In one of the very few cases on this issue a man was convicted of criminal damage to his ex-girlfriend's Facebook page and fined €2,000 after he used her phone to log into her account and post a status update in her name saying that she was a 'whore' – the fine reflecting the reputational harm rather than any monetary or proprietary damage (Barrett and Mishkin, 2014).

System interference

Article 5 of the Convention requires states to establish offences relating to the 'serious hindering without right of the functioning of a computer system'. This addresses denial of service attacks, which aim to prevent users from accessing a particular website or service, usually by flooding servers with traffic in a way which prevents them from functioning by using up bandwidth, processing power or storage capacity. The most common variant is the distributed denial of service attack, which uses a large number of compromised computers as the springboard for the attack (Burden and Palmer, 2003; Houle and Weaver, 2001).

There is no direct counterpart to article 5 in Irish law, meaning that any denial of service attack could only be prosecuted indirectly. For example, suppose that A sets out to hinder communications with B by sending several million emails to B. The effect is not only to use up B's bandwidth but also to use up his storage capacity. In this case, it might be possible to charge A with criminal damage under section 2 of the Criminal Damage Act 1991, on the basis that A has damaged B's data within the meaning of section 1 by adding to it without lawful excuse.¹² It is, however, undesirable to rely on this roundabout way of prosecuting as slight variations in the structure of attacks may mean that there is no appropriate offence to charge.

Misuse of devices

Article 6 of the Cybercrime Convention requires states to establish secondary offences relating to the production, sale, possession, distribution, etc. of 'hacking tools' and passwords or access codes. This aims to reduce cybercrime by limiting the availability of these tools on the 'black market', supposedly making it more difficult for attacks to be carried out (Council of Europe, 2001, para. 71).

This is an extremely controversial provision, often criticised as based on a simplistic belief that it is possible to categorise software as inherently good or evil. Instead, as Sommer notes "the difficulty is that many hacking tools are indistinguishable from utilities that are essential for the maintenance and security of computers and networks" (Sommer, 2006, p. 68). Consequently, there is concern that poorly drafted 'hacking tool' laws may criminalise the work of researchers and other professionals in information security (McEwan, 2008).

¹² Compare the English decision in *DPP v. Lennon* [2006] EWHC 1201 holding that while a public email address carries an implied consent to receive emails this does not extend to emails which are deliberately sent to disrupt a system.

While Irish law does not specifically deal with ‘hacking tools’ and passwords, it may be possible to prosecute in individual cases using section 4 of the Criminal Damage Act 1991. That section provides:

A person (in this section referred to as the possessor) who has any thing in his custody or under his control intending without lawful excuse to use it or cause or permit another to use it ... to damage any property belonging to some other person ... shall be guilty of an offence.

Bearing in mind that the definition of property under the 1991 Act includes data, this section may be wide enough to criminalise possession of software which is intended to damage data.¹³ But note that this section does not criminalise creation, possession, sale or distribution *per se* – in every case it must be shown that the defendant had an intention to use the item to damage data (or to allow another person to do so). This creates two related problems for prosecutors. From an evidential point of view, they will face a difficulty in demonstrating that an accused person had the necessary intention. Moreover, the intention which must be shown is an intention to damage property – a mere intention to carry out an unauthorised access would not suffice. If, for example, A were found to be in possession of a username and password belonging to B, this would not be an offence under section 4 if A’s intention was merely to view B’s data.

Computer-related offences

Computer-related forgery

The first ‘computer-related’ offence provided for by the Convention is computer-related forgery.¹⁴ The Explanatory Report to the Cybercrime Convention summarises this as ‘creating a parallel offence to the forgery of tangible documents’ to fill “gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data” (Council of Europe, 2001, para. 81). It is largely addressed in Irish law by forgery under section 25 of the Criminal Justice (Theft and Fraud Offences) Act 2001, which provides:

A person is guilty of forgery if he or she makes a false instrument with the intention that it shall be used to induce another person to accept it as genuine and, by reason of so accepting it, to do some act, or to make some omission, to the prejudice of that person or any other person.

The 2001 Act was drafted with computer crime in mind, and consequently section 24 defines ‘instrument’ in a way which is intended to be technology neutral as including any “disk, tape, sound track or other device on or in which information is recorded or stored by mechanical, electronic or other means”. Similarly, section 31(3) deals with the requirement that a person be deceived by providing that inducing a person to accept an item as genuine will include “inducing a machine to respond to the instrument... as if it were a genuine instrument”.

Computer-related fraud

¹³ Assuming that “thing” is wide enough to cover software as well as tangible items.

¹⁴ Article 7.

The offence of computer related fraud under article 8 of the Convention roughly corresponds to the offence of dishonest use of a computer under section 9 of the Criminal Justice (Theft and Fraud Offences) Act 2001, which provides:

A person who dishonestly, whether within or outside the State, operates or causes to be operated a computer within the State with the intention of making a gain for himself or herself or another, or of causing loss to another, is guilty of an offence.

On its face this appears to be a very far-reaching provision which would cover most situations where “a person lawfully has a computer but uses it for a dishonest purpose”.¹⁵ However, ambiguous drafting means that when examined more closely the offence may be narrower. The offence is committed only where a person dishonestly operates a computer. Dishonesty is defined in section 2 to mean “without a claim of right made in good faith”. Consequently (while the section is not entirely clear) it appears to apply only where a person operates a computer without a claim of right made in good faith – that is, without authorisation. If, for example, A uses his own computer to print a forged cheque, this would be a ‘dishonest use of a computer’ in a colloquial sense but would not be operation of a computer without a claim of right as required by this offence.

Content-related offences

Article 9 of the Cybercrime Convention requires states to establish offences relating to the producing, making available, distributing, procuring and possession of child pornography through computer systems. These are largely already covered by the Child Trafficking and Pornography Act 1998. That act was generally viewed as forward looking for its time – for example, in providing technology neutral definitions of offences and avoiding subjective terms such as ‘obscene’, ‘indecent’ and ‘offensive’ – and has largely been unproblematic in practice (Clark and Hyland, 2007, chap. 4; O’Donnell and Milner, 2007, chap. 4 and 6).

That said, a number of changes are needed to take account of new trends in offending – for example, a shift away from downloading and possession of images and towards streaming video and even live footage of children being abused. These changes have been addressed at international level by the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse¹⁶ and by Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography. In 2014 the Department of Justice published a general scheme of a Sexual Offences Bill which will implement the Directive and enable the Convention to be ratified. This will, for example, extend the 1998 Act to criminalise ‘obtaining access to child pornography’, making it an offence to watch a streaming video as well as to possess such a video (Department of Justice and Equality, 2014).

Offences related to infringements of copyright and related rights

Article 10 of the Cybercrime Convention requires states to criminalise certain infringements of copyright and related rights where these are committed “wilfully, on

¹⁵ See the comments of the Minister for Justice at 168 *Seanad Debates* Col. 1130.

¹⁶ CETS no. 201.

a commercial scale and by means of a computer system”. This is done in the Republic of Ireland by section 140 of the Copyright and Related Rights Act 2000 which predates the Convention and criminalises the making for sale, selling, making available in the course of a business, etc. of infringing copies of works (Clark et al., 2010, pp. 417–421). This section has most commonly been used to prosecute tangible infringements – pirated copies of DVDs and CDs for example – and there does not appear to be any reported case of it being used in the Republic of Ireland to prosecute copyright infringement online.

Other offences

One limitation of the Cybercrime Convention is that it is primarily focused on crimes against property and crimes of dishonesty. Apart from child abuse images it does not specifically address crimes against the individual. However two such cybercrimes are particularly topical and should be mentioned also – disclosure of personal data and online harassment.

Disclosure of personal data

There is a widespread problem in the Republic of Ireland where individuals in large organisations – including state bodies such as Revenue, the Garda Síochána and the Department of Social Protection – abuse their access to databases of sensitive personal information (Kennedy, 2012; Tighe, 2011; Brady, 2014; O’Connor, 2014; Kennedy, 2011). In addition to simple snooping this has included passing on information to private investigators and others. Historically, these cases have not generally been dealt with using the criminal law but as we have already seen the DPC has begun to prosecute a number of cases involving private investigators.

The most important offence in these cases is section 22 of the Data Protection Acts 1988 and 2003 which provides that a person is guilty of an offence if they (a) obtain access to personal data without the authority of the data controller or data processor by whom it is kept, and (b) disclose that data to another person. This will include obtaining data by ‘blagging’ or ‘pretexting’ – that is, extracting information by pretending to be a person with a legitimate need for the information.

However the limitations of that offence must be noted. First, it applies to outsiders only – subsection (2) excludes “a person who is an employee or agent of the data controller or data processor concerned”. It does not address insiders who snoop, though it is possible that they might be guilty of unauthorised access by doing so. Second, it requires onward disclosure of the information. It is not an offence under section 22 to obtain personal data if it is not then passed on to a third party.¹⁷ Finally, and perhaps most importantly, the sanctions may not be adequate to deter what has become a very lucrative business. Section 22 does not carry a custodial sentence, and as a practical matter will almost always be prosecuted in the District Court where fines will be relatively low – indeed, in a number of cases the Probation Act has been applied (Brennan, 2011; Edwards, 2014; McGuire, 2014; Tuite and Kennedy, 2012). The introduction of custodial sentences for the equivalent offence has been recommended

¹⁷ Compare section 55(1) of the UK Data Protection Act 1998 which criminalises simple obtaining of personal data, subject to some exceptions.

in the United Kingdom and could be considered here also, even if only at the summary level (Society for Computers and Law, 2012).

Harassment and cyberbullying

Online harassment or ‘cyberbullying’ has become more common in recent years with the growth in social media and there has been particular concern about its prevalence amongst children (O’Neill et al., 2011; O’Neill and Dinh, 2013). It has been an emotive and high profile issue in the Republic of Ireland since late 2012, when the suicides of two teenage girls were linked to comments made about them on social media. Since then we have seen the issue considered by the Oireachtas Joint Committee on Transport and Communications (2013), the Special Rapporteur on Child Protection (2013), the Internet Content Advisory Group (2014), and most recently the Law Reform Commission (2014).

In each of these contexts largely the same questions are being asked. To what extent should the law criminalise crude or offensive speech online? Should the law differentiate between messages directed *to* a person and messages *about* a person? Is the criminal law an appropriate response to misbehaviour by children themselves? Are civil law remedies adequate to protect against harassment and to respond to invasions of privacy? How should the law deal with so-called ‘revenge pornography’, or as it is more accurately termed ‘non-consensual distribution of private sexual images’ (McGlynn and Rackley, 2014)? What procedures should be in place to identify individuals who post messages anonymously or pseudonymously? Is this an area best addressed by legal controls, technological measures such as user blocking and/or private policing by social media firms?

Without entering into the current debate in detail, we should note that the criminal offence currently most often used to prosecute cyberbullying is section 10 of the Non-Fatal Offences Against the Person Act 1997. This creates an offence of harassment and prohibits the harassment of a person ‘by any means’ by ‘persistently following, watching, pestering, besetting or communicating with him or her’. The reference to communication ‘by any means’ is technology neutral and permits prosecutions to be brought where the harassment takes place electronically. While the crime statistics do not break out cases of online harassment, a search of newspaper archives reveals many cases where defendants have been convicted of harassment by email, text messages, tweets and even indirectly by posting fake posts in the name of the victim (Cunningham, 2010; Fallon, 2014; Magee and Ferguson, 2014). While there have been some claims that the substantive law is inadequate to address online harassment, these are belied by the number of successful prosecutions which have been brought. Instead, it seems more likely that the main obstacle may be a lack of resources to pursue these cases.

That said, there is nevertheless a possible issue with this offence in the requirement that the harassment be ‘persistent’. While this is important in setting a threshold of seriousness, it may mean that some grave harms escape its scope. Consider, for example, a once-off public posting of private sexual images. This would not meet the persistence requirement, notwithstanding that it would be experienced as extremely humiliating and demeaning. There is a good case for a separate crime to deal with this

type of exposure of private material, as in the new English offence of disclosing private sexual photographs and films with intent to cause distress.¹⁸

Mandatory reporting of cybercrime

A significant and distinctive aspect of Irish law is the way in which it increasingly provides for mandatory reporting of crimes. Although the common law offence of misprision of felony (failing to report a felony) was repealed in 1997¹⁹ it has since been largely replaced with specific statutory duties to report serious offences against the person or property²⁰, offences against children and other vulnerable persons²¹ and, most importantly for our purposes, the majority of crimes of dishonesty and cybercrimes.²²

The duty to report cybercrimes is contained in section 19 of the Criminal Justice Act 2011, which was adopted following the Irish banking crisis. It creates a criminal offence where a person fails to volunteer information to police, as follows:

A person shall be guilty of an offence if he or she has information which he or she knows or believes might be of material assistance in—
(a) preventing the commission by any other person of a relevant offence, or
(b) securing the apprehension, prosecution or conviction of any other person for a relevant offence,
and fails without reasonable excuse to disclose that information as soon as it is practicable to do so to a member of the Garda Síochána.

What crimes must be reported? The duty relates to ‘relevant offences’, a term defined exceptionally widely to include approximately 130 crimes.²³ These range from insider dealing and market manipulation offences to simple theft. Although the expressed aim of the 2011 Act was to deal with complex white collar crime, this provision goes significantly further and includes essentially all crimes of dishonesty. Crucially, Schedule 2 specifically includes dishonest use of a computer²⁴ and criminal damage to data²⁵ in its scope.

The effect of the 2011 Act is that mandatory reporting will now apply to almost all cybercrimes involving dishonesty or cybercrimes where the computer is a target (apart from simple unauthorised access or disclosure of data). For example, fraud by an employee using a computer system, 419 fraud emails, phishing emails and the use of trojans, ransomware or other malware will all constitute one or other relevant offences.

This creates a remarkably invasive though often underappreciated duty. It applies to ‘all persons’ – unlike other reporting obligations which may be limited to certain professions or positions – and applies to the victims of cybercrime themselves. It is prospective as well as retrospective – it applies to information which might prevent the

¹⁸ Section 33, Criminal Justice and Courts Act 2015. There is, as yet, no equivalent offence in Northern Ireland.

¹⁹ Section 3, Criminal Law Act 1997.

²⁰ Section 9, Offences Against the State (Amendment) Act 1998.

²¹ Section 2, Criminal Justice (Withholding of Information on Offences Against Children and Vulnerable Persons) Act 2012.

²² Section 19, Criminal Justice Act 2011.

²³ Schedule 2.

²⁴ Section 9, Criminal Justice (Theft and Fraud Offences) Act, 2001.

²⁵ Criminal Damage Act 1991.

commission of future offences as well as information which might assist in prosecuting past offences. It applies to information which ‘might’ be of material assistance, not merely information of clear importance. It is not limited to responding to questioning but creates an affirmative obligation to volunteer information to a garda ‘as soon as is practicable’. It also leaves undefined what might constitute a ‘reasonable excuse’ for failure to provide information.

The constitutionality of this provision has been questioned by McDowell (2011) but so long as it remains in force it will have a significant effect in the area of cybercrime. At a practical level it has led to a large number of reports being made to gardaí on a precautionary basis, leading to complaints that the GBFI has been ‘swamped’ with information which it cannot use (McDonald, 2014).

It also has significant implications for criminological and information security research in this area, where it is now unclear when researchers must volunteer information to gardaí and to what extent assurances of confidentiality might be given to subjects. In light of the 2011 Act, it is questionable whether, for example, researchers based in this jurisdiction could replicate the ethnographic work carried out by Coleman (2014) who studied the Anonymous movement through close and frequent contact with its members. By talking to those who have committed or might commit cybercrimes, researchers in many cases will place themselves in a position of having information which ‘might be of material assistance’ to gardaí with no certainty as to whether they have a ‘reasonable excuse’ for failing to report that information. There is every possibility that this provision will make the Irish internet less rather than more secure by acting as a deterrent to research into cybercrime.

Duty to report data breaches

A separate duty to report should also be mentioned. There is an international trend in the area of data protection law to require that individuals and regulators should be notified of security breaches affecting personal data. In the European Union, this is now mandatory in the case of breaches in the telecommunications sector and if the current proposed Data Protection Regulation is adopted it will be extended to data breaches in other industries also (Burdon et al., 2012; Wong, 2013, chap. 6). This is not a duty to report crime *per se* – it applies equally to simple carelessness resulting in the loss of personal data – but it will nevertheless apply to many types of cybercrime where user information is put at risk.

Conclusion

The aim of this chapter has been to provide a brief survey of the key aspects of cybercrime in the Republic of Ireland. At the level of the substantive law, the overall picture is one of a confused statutory landscape, in which many of the substantive offences are essentially *ad hoc*, tacked on to unrelated legislation and lacking consistency with each other. This is exacerbated by the small number of prosecutions brought and an almost complete lack of reported judgments. In many cases, newspaper reports of cases are the only materials available to assess how the offences have been interpreted in practice, and there is still a level of ambiguity as to basic elements of the offences. The forthcoming legislation to implement the Directive on attacks against Information Systems and to enable ratification of the Cybercrime Convention

represents a rare opportunity to bring coherence to this area and it is disappointing that it has not been the subject of any public consultation.

Looking at the wider context, there is a clear need for more research into the prevalence of cybercrime in the Republic of Ireland. The Police Service of Northern Ireland now provides separate statistics for crimes which were committed in whole or in part through a computer or computer network and it would be desirable for the Garda Síochána to follow this lead (Young, 2014). As regards the policing of cybercrime, more work needs to be done on the way in which the Garda investigates cybercrime and the division of responsibilities between the CCIU/PIU and local investigations. While some reform of the law is undoubtedly necessary, the 2014 Garda Inspectorate report suggests that the most pressing need is for more resources rather than more laws.

Bibliography

- Akdeniz, Yaman. Freedom of Expression on the Internet: Study of Legal Provisions and Practices Related to Freedom of Expression, the Free Flow of Information and Media Pluralism on the Internet in OSCE Participating States. Organisation for Security and Cooperation in Europe, 2011. <http://www.osce.org/fom/80723>.
- Anderson, Ross, Chris Barton, Rainer Bohme, Richard Clayton, Michel JG van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. "Measuring the Cost of Cybercrime." Berlin, 2012. http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.
- Barrett, Claer, and Sarah Mishkin. "Ex-Boyfriend Fined €2,000 for Facebook 'frape.'" Financial Times, July 2, 2014. <http://www.ft.com/cms/s/0/186f95d6-01d4-11e4-bb71-00144feab7de.html>.
- Brady, Tom. "Gardai Checked Private Files on Model More than 80 Times." Irish Independent, March 22, 2014. <http://www.independent.ie/irish-news/gardai-checked-private-files-on-model-more-than-80-times-30115460.html>.
- Brennan, Declan. "Insurer's Private Eye Admits Tax Data Breach." Irish Independent, December 17, 2011. <http://www.independent.ie/irish-news/insurers-private-eye-admits-tax-data-breach-26803048.html>.
- Brenner, Susan W. "Is There Such a Thing as 'Virtual Crime'?" Berkeley Journal of Criminal Law 4, no. 1 (2001): 3.
- Burden, Kit, and Creole Palmer. "Internet Crime: Cyber Crime - A New Breed of Criminal?" Computer Law and Security Report 19, no. 3 (2003): 222.
- Burdon, Mark, Bill Lane, and Paul von Nessen. "Data Breach Notification Law in the EU and Australia – Where to Now?" Computer Law & Security Review 28, no. 3 (June 2012): 296–307.
- Casey, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Academic Press, 2011.
- Central Statistics Office. Garda Recorded Crime Statistics. Dublin, 2014. http://www.cso.ie/en/media/csoie/releasespublications/documents/crimejustice/2012/gardacrimestats_2012.pdf.
- . Irish Crime Classification System, 2008. <http://www.cso.ie/en/media/csoie/releasespublications/documents/crimejustice/current/crimeclassification.pdf>.
- Clark, Robert. "Computer Related Crime in Ireland." European Journal of Crime, Criminal Law and Criminal Justice 2 (1994): 252.

- Clark, Robert, and Mark Hyland. *The Criminalisation of Child Pornography in Irish Law: A Report to the Department of Justice, Equality and Law Reform*. Dublin: School of Law, University College Dublin, June 2007. <http://papers.ssrn.com/abstract=1393309>.
- Clark, Robert, Shane Smyth, and Niamh Hall. *Intellectual Property Law in Ireland*. 3rd ed. Dublin: Bloomsbury Professional, 2010.
- Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Verso Books, 2014.
- Conway, Maura. "Terrorism and the Internet: New Media--New Threat?" *Parliamentary Affairs* 59, no. 2 (2006): 283–98.
- Council of Europe. "Explanatory Report to the Convention on Cybercrime (ETS No. 185)," 2001. <http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm>.
- Cunningham, Gerard. "Dad Is Guilty of Hounding Professor in Emails Blitz." *Evening Herald*, April 16, 2010. <http://www.herald.ie/news/dad-is-guilty-of-hounding-professor-in-emails-blitz-27948733.html>.
- Data Protection Commissioner. *Annual Report 2007*. Dublin, 2008. <http://www.dataprotection.ie/documents/annualreports/AR2007En.pdf>.
- Deloitte. *Irish Information Security and Cybercrime Survey 2013*. Dublin, 2013. https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/cybercrime_survey_risk_2013_deloitte_ireland.pdf.
- Demeyer, Karel, Eva Lievens, and Jos Dumortier. "Blocking and Removing Illegal Child Sexual Content: Analysis from a Technical and Legal Perspective." *Policy & Internet* 4, no. 3–4 (2012): 1.
- Department of Justice and Equality. "Heads of Criminal Law (Sexual Offences) Bill 2014," 2014. <http://www.justice.ie/en/JELR/Pages/PR14000349>.
- Duncan, Pamela. "Garda and UPC Agreement Will Restrict Access to Sites with Child Porn Images." *Irish Times*, November 11, 2014. <http://www.irishtimes.com/news/ireland/irish-news/garda-and-upc-agreement-will-restrict-access-to-sites-with-child-porn-images-1.1995687>.
- Edwards, Elaine. "Private Investigator Fined €5,000 for Accessing Garda Data." *Irish Times*, November 24, 2014. <http://www.irishtimes.com/news/crime-and-law/private-investigator-fined-5-000-for-accessing-garda-data-1.2012999>.
- Edwards, Lilian. "Pornography, Censorship and the Internet." In *Law and the Internet*, edited by Lilian Edwards and Charlotte Waelde, 3rd ed. Oxford: Hart Publishing, 2009.
- Edwards, Lilian, Judith Rauhofer, and Majid Yar. "Recent Developments in UK Cybercrime Law." In *Handbook of Internet Crime*, edited by Yvonne Jewkes and Majid Yar, 413–36. Cullompton: Willan, 2010.
- Fallon, John. "Man Who Posted 'vile Messages' to Ex-Girlfriend Avoids Jail." *Irish Examiner*, March 20, 2014. <http://www.irishexaminer.com/ireland/man-who-posted-vile-messages-to-ex-girlfriend-avoids-jail-262520.html>.
- Galetsas, Antonis. *Statistical Data on Network Security*. Brussels: European Commission, March 5, 2007. ftp://ftp.cordis.europa.eu/pub/ist/docs/trust-security/statistics-network-security-050307_en.pdf.
- Gallagher, Eugene. "The State's Response to the Threats Posed by Cyber-Crime – Is It Adequate or Ineffectual?" *Communique: Management Journal of an Garda Síochána*, December 2005, 20.
- Garda Síochána Inspectorate. *Crime Investigation*. Dublin, October 2014. http://www.gsinsp.ie/index2.php?option=com_docman&task=doc_view&gid=243&Itemid=152.

- Grabosky, Peter N. "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10, no. 2 (June 1, 2001): 243–49.
- Grigsby, Alex. "Coming Soon: Another Country to Ratify the Budapest Convention." *Council on Foreign Relations - Net Politics*, December 11, 2014. <http://blogs.cfr.org/cyber/2014/12/11/coming-soon-another-country-to-ratify-to-the-budapest-convention/>.
- GSMA. "GSMA Launches Mobile Alliance Against Child Sexual Abuse." *GSM World*, February 11, 2008. <http://www.gsmworld.com/newsroom/press-releases/2008/775.htm>.
- GSMA Mobile Alliance Against Child Sexual Abuse Content. "Implementation of Filtering of Child Sexual Abuse Images in Operator Networks," November 2008. www.gsmworld.com/documents/GSMA_Child_Tech_Doc.pdf.
- Hall, Eamonn. *The Electronic Age: Telecommunications in Ireland*. Dublin: Oak Tree Press, 1993.
- Houle, Kevin, and George Weaver. *Trends in Denial of Service Attack Technology*. Pittsburgh: CERT Coordination Centre, October 2001. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52490>.
- Internet Content Governance Advisory Group. *Report of the Internet Content Governance Advisory Group*. Dublin: Department of Communications, Energy and Natural Resources, 2014. <http://www.dcenr.gov.ie/NR/rdonlyres/0BCE1511-508E-4E97-B1A9-23A6BE9124AA/0/InternetContentGovernanceAdvisoryGroup.pdf>.
- Internet Service Providers Association of Ireland. *Hotline.ie Annual Report 2013*. Dublin, 2014. <http://www.hotline.ie/2013/report2013.pdf>.
- Jewkes, Yvonne, and Carol Andrews. "Policing the Filth: The Problems of Investigating Online Child Pornography in England and Wales." *Policing & Society* 15, no. 1 (March 2005): 42.
- Joint Committee on Transport and Communications. *Addressing the Growth of Social Media and Tackling Cyberbullying*. Dublin: Houses of the Oireachtas, July 2013. <http://www.oireachtas.ie/parliament/media/Report-on-Social-Media-July-2013-Website.pdf>.
- Kehoe, Paul. "Government Legislation Programme Spring/Summer 2015." *Department of the Taoiseach*, January 14, 2015. http://www.taoiseach.gov.ie/eng/Taoiseach_and_Government/Government_Legislation_Programme/Government_Legislative_Programme_Spring_Summer_2015.pdf.
- Kelleher, Denis. *Privacy and Data Protection Law in Ireland*. Dublin: Tottel, 2006.
- Kelleher, Denis, and Karen Murray. *Information Technology Law in Ireland*. 2nd ed. Dublin: Tottel, 2007.
- Kennedy, Edel. "Gardai Probe Revenue Officials over Tax Scam." *Irish Independent*, January 1, 2011. <http://www.independent.ie/irish-news/gardai-probe-revenue-officials-over-tax-scam-26610277.html>.
- . "Snooping Civil Servants Who Gave out Personal Data Keep Their Jobs." *Irish Independent*, February 15, 2012. <http://www.independent.ie/irish-news/snooping-civil-servants-who-gave-out-personal-data-keep-their-jobs-26821880.html>.
- Kirwan, Gráinne, and Andrew Power. *Cybercrime: The Psychology of Online Offenders*. Cambridge University Press, 2013.
- . "Hacking: Legal and Ethical Aspects of an Ambiguous Activity." In *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices*,

- edited by Alfreda Dudley, James Braman, and Giovanni Vincenti. IGI Global, 2011. <http://www.igi-global.com/chapter/hacking-legal-ethical-aspects-ambiguous/59935>.
- Koops, Bert-Jaap, and Tessa Robinson. "Cybercrime Law." In *Digital Evidence and Computer Crime*, edited by Eoghan Casey, 3rd ed. Waltham, MA: Academic Press, 2011.
https://pure.uvt.nl/portal/files/1332174/Koops_Cybercrime_Law_European_Perspective_110525_postprint_embargo_1_y.pdf.
- Laidlaw, Emily. "The Responsibilities of Free Speech Regulators: An Analysis of the Internet Watch Foundation." *International Journal of Law and Information Technology* 20, no. 4 (2012): 312.
- Law Reform Commission. *Issues Paper on Cyber-Crime Affecting Personal Safety, Privacy and Reputation Including Cyber-Bullying*, 2014.
http://www.lawreform.ie/_fileupload/Issues%20Papers/ip6Cybercrime.pdf.
- Licken, Eoin. "Case Prompts Fears over Web Use." *Irish Times*, August 14, 1998.
http://www.irishtimes.com/newspaper/finance/1998/0814/98081400196_pf.html.
- Magee, Jessica, and Fiona Ferguson. "Woman in Custody after Harassing Wife of Former Colleague." *Independent.ie*, July 10, 2014.
<http://www.independent.ie/irish-news/courts/woman-in-custody-after-harrassing-wife-of-former-colleague-30422355.html>.
- McDonald, Dearbhail. "There's Never Been a Better Time for White-Collar Crime, Warns Lawyer." *Irish Independent*, June 2, 2014.
<http://www.independent.ie/irish-news/theres-never-been-a-better-time-for-whitecollar-crime-warns-lawyer-30321343.html>.
- McDowell, Michael. "Law Means We Are All Informers." *Irish Independent*, August 21, 2011. <http://www.independent.ie/opinion/analysis/law-means-we-are-all-informers-26763354.html>.
- McEwan, Neil. "The Computer Misuse Act 1990: Lessons from Its Past and Predictions for Its Future." *Criminal Law Review*, 2008, 955.
- McGlynn, Clare, and Erika Rackley. *Revenge Pornography Briefing*. Durham, July 7, 2014.
<https://www.dur.ac.uk/resources/glad/RevengePrnBriefingMcGlynnRackleyJuly2014.pdf>.
- McGuire, Erin. "Private Investigators Admit 'blagging' Credit Union Data." *The Irish Times*, October 6, 2014. <http://www.irishtimes.com/news/crime-and-law/courts/private-investigators-admit-blagging-credit-union-data-1.1953874>.
- McGuire, Michael, and Samantha Dowling. *Cyber Crime: A Review of the Evidence*. London: Home Office, October 2013.
<https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence>.
- McIntyre, T.J. "Child Abuse Images and Cleanfeeds: Assessing Internet Blocking Systems." In *Research Handbook on Governance of the Internet*, edited by Ian Brown. Cheltenham: Edward Elgar, 2013.
- . "Computer Crime in Ireland: A Critical Assessment of the Substantive Law." *Irish Criminal Law Journal* 15, no. 1 (2005): 13.
- . "Cybercrime in Ireland." In *Cybercrime and Security*, edited by Pauline C. Reich. Oxford University Press, 2008.

- McMahon, Aine. "Data Protection Gets Funding Doubled." *Irish Times*, December 18, 2014. <http://www.irishtimes.com/news/politics/data-protection-gets-funding-doubled-1.2043073>.
- Mooney, John. "Garda Computer Backlog Leads to Three-Year Delay in Child Porn Cases." *The Sunday Times*, May 18, 2014. <http://www.thesundaytimes.co.uk/sto/news/ireland/article1412168.ece>.
- Murray, Karen. "Computer Misuse Law in Ireland." *Irish Law Times* 13 (1995): 114.
- . "The Criminal Justice (Theft and Fraud Offences) Bill 2000 and the Internet." *Irish Law Times* 19 (2001): 143.
- Northern Ireland Policing Board. *Public Confidence in the Policing of Cybercrime*. Belfast, 2014. <http://www.nipolicingboard.org.uk/news/article.htm?id=15529>.
- O'Connor, Niall. "Probe into Civil Servant Who Snooped on Dozens of Women for 'Curiosity.'" *Irish Independent*, August 18, 2014. <http://www.independent.ie/irish-news/news/probe-into-civil-servant-who-snooped-on-dozens-of-women-for-curiosity-30514979.html>.
- O'Connor, Owen. *2nd ISSA / UCD Irish Cybercrime Survey*. Dublin: University College Dublin, 2008.
- O'Connor, Owen, and Pavel Gladyshev. *ISSA / UCD Irish Cybercrime Survey*. Dublin: University College Dublin, 2006. http://www.ucd.ie/cc/news_and_events/publications/issa_ucd_irish_cybercrime_survey_2006.pdf.
- O'Donnell, Ian, and Claire Milner. *Child Pornography: Crime, Computers and Society*. Cullompton: Willan, 2007.
- O'Neill, Brian, and Thuy Dinh. *Cyberbullying among 9-16 Year Olds in Ireland*. Digital Childhoods Working Paper Series. Dublin: Dublin Institute of Technology, 2013. <http://arrow.dit.ie/cserrep/31/>.
- O'Neill, Brian, Simon Grehan, and Kjartan Ólafsson. *Risks and Safety for Children on the Internet: The Ireland Report*. London: LSE, February 8, 2011. <http://arrow.dit.ie/cserrep/22>.
- Special Rapporteur on Child Protection. *Sixth Report*, January 2013. <http://www.dcy.gov.ie/documents/Publications/SixthRapporteurReport.pdf>.
- Prins, Corien. "Should ICT Regulation Be Undertaken at an International Level?" In *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, edited by Bert-Jaap Koops, Miriam Lips, Corien Prins, and Maurice Schellekens. *Information Technology and Law* 9. The Hague: T.M.C. Asser Press, 2006.
- PwC. *Economic Crime: A Persisting Threat in Ireland*. Dublin, 2014. <http://download.pwc.com/ie/pubs/2014-pwc-irish-economic-crime-survey.pdf>.
- Reilly, Gavan. "Two out of Five Garda Stations Don't Have Email Access." *TheJournal.ie*, February 12, 2012. <http://www.thejournal.ie/two-out-of-five-garda-stations-dont-have-email-access-353291-Feb2012/>.
- Riley, M.C. "Anarchy, State, or Utopia?: Checks and Balances in Internet Governance." *IEEE Internet Computing* 17, no. 3 (2013): 10–17. doi:10.1109/MIC.2013.24.
- Rogers, Stephen. "Garda Child Porn Forensics Unit to Get Extra Staff." *Irish Examiner*, July 14, 2014. <http://www.irishexaminer.com/ireland/garda-child-porn-forensics-unit-to-get-extra-staff-275343.html>.
- Ryan, Pearse, and Andy Harbison. "The Law on Computer Fraud in Ireland – Development of the Law and Dishonesty." *Computers and Law*, June 2010.

- Ryan, Pearse, Claire O'Brien, and Andy Harbison. "Cybercrime in Ireland – Recent Legislative Developments." *Computers and Law*, 2013.
- Smith, Gordon. "Cybercrime Victims Urged to Enlist Police Help." *SiliconRepublic.com*, April 1, 2005. <http://www.siliconrepublic.com/enterprise/item/4333-cybercrime-victims-urged-to>.
- Society for Computers and Law. "Blagging Convictions: Comments from the ICO." *Computers and Law*, February 27, 2012. <http://www.scl.org/site.aspx?i=ne25223>.
- Sommer, Peter. "Criminalising Hacking Tools." *Digital Investigation* 3, no. 2 (2006): 68–72.
- Stack, Sarah. "Students Who Hacked the Fine Gael Website Hand over €5,000 Each." *Irish Independent*, October 8, 2013. <http://www.independent.ie/irish-news/courts/students-who-hacked-the-fine-gael-website-hand-over-5000-each-29643575.html>.
- Stack, Sarah, and Ed Carty. "Gardaí Picket Closed-Door Talks over Public-Sector Pay." *Irish Independent*, February 21, 2013. <http://www.independent.ie/irish-news/gardai-picket-closeddoor-talks-over-publicsector-pay-29086220.html>.
- Stol, Wouter, Rik Kaspersen, Joyce Kerstens, Rutger Leukfeldt, and Arno Lodder. "Governmental Filtering of Websites: The Dutch Case." *Computer Law & Security Review* 25 (2009): 251.
- Taylor, Max, and Ethel Quayle. *Child Pornography: An Internet Crime*. Hove: Brunner-Routledge, 2003.
- . "Criminogenic Qualities of the Internet in the Collection and Distribution of Abuse Images of Children." *Irish Journal of Psychology* 29, no. 1–2 (2008): 119.
- Tighe, Mark. "Garda Accused of Bugging Her Ex-Boyfriend." *The Sunday Times*, February 20, 2011.
- TNS Opinion & Social. *Eurobarometer 423: Cyber Security*. Brussels: European Commission, 2015. http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf.
- Tuite, Tom. "Civil Servant Who Hacked Boss's Phone Walks Free." *Irish Independent*, May 24, 2013. <http://www.independent.ie/irish-news/courts/civil-servant-who-hacked-bosss-phone-walks-free-29294982.html>.
- Tuite, Tom, and Edel Kennedy. "Data Leak Insurers Escape Criminal Conviction." *Irish Independent*, March 6, 2012. <http://www.independent.ie/irish-news/courts/data-leak-insurers-escape-criminal-conviction-26828814.html>.
- UPC. "Press Release: UPC First Major ISP to Introduce Safeguard Measures for Child Sexual Abuse Material," November 10, 2014. <http://www.upc.ie/pdf/pressrelease/safeguard-measures.pdf>.
- Van Turnhout, Jillian. "Online Child Abuse Material: Effective Strategies to Tackle Online Child Abuse Material," September 2013. <https://www.scribd.com/doc/169316613/Van-Turnhout-Report-Effective-Strategies-to-Tackle-Online-CAM-Sept-2013>.
- Wall, David. *Cybercrime: The Transformation of Crime in the Information Age*. Polity, 2007.
- . "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace." *Police Practice & Research: An International Journal* 8, no. 2 (2007): 183–205.

- Wong, Rebecca. *Data Security Breaches and Privacy in Europe*. Springer, 2013.
- Working Group on the Illegal and Harmful Use of the Internet. *Illegal and Harmful Use of the Internet: First Report of the Working Group*. Dublin: The Stationery Office, 1998.
http://ec.europa.eu/avpolicy/docs/reg/minors/useinternet1streport_ie.pdf.
- Yar, Majid. "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory." *European Journal of Criminology* 2, no. 4 (October 1, 2005): 407–27.
- . "The Private Policing of Internet Crime." In *Handbook of Internet Crime*, edited by Yvonne Jewkes and Majid Yar. Routledge, 2010.
- Young, David. "Police's 'Pop-up Shop' to Advise Public over Online Crime Threat." *BelfastTelegraph*, November 28, 2014.
<http://www.belfasttelegraph.co.uk/news/northern-ireland/polices-popup-shop-to-advise-public-over-online-crime-threat-30780943.html>.