

CYBERCRIME INVESTIGATION AND PROSECUTION – SHOULD IRELAND RATIFY THE CYBERCRIME CONVENTION?

ADRIAN BANNON

I. INTRODUCTION

The issue of what is known as computer crime and the adoption of a unified approach across the international territory has been a prominent legal issue, particularly among the G8 states in recent years. This paper, therefore, endeavours to interpret the amorphous concept of computer crime and the likely impacts (if any) that state ratification of the recently adopted convention on cybercrime may have regarding the law on this issue.

“The proliferation and integration of computers into every aspect of society has inevitably led to computer-related criminal activities.”¹ Such an information revolution has created a technologically dependent society. Consequently, in this “Age of the Internet,” access to information is unprecedented. This access can be positively used or negatively used to gain unauthorised access to information or to steal profitable data.²

The Internet is a network of computers communicating with each other on the bases of the Transport Control Protocol/Internet Protocol (TCP/IP). It is an international network of interconnected computers, which enables millions of people to communicate with one another in “cyberspace” and to access vast amounts of information from around the world.³ The very notion of sharing and receiving information is central to the ethos of the Internet.⁴ In this era, immense damage can be done by an individual sitting halfway around the world. The openness of the Internet

¹ Reed & Angel (eds.) *Computer Law* (Oxford University Press, 2003) at p. 295.

² Kennedy, “In Search of a Balance between Police Power and Privacy in the Cybercrime Treaty,” 9 *Richmond Journal of Law & Technology* 3 (2002).

³ Cronin, “An analysis of the Irish Data Protection Law in relation to the protection of privacy in the online environment” [2003] *Cork Online Law Review*, available at <http://colr.ucc.ie/review03.htm>.

⁴ *Ibid.* at *3.

renders it vulnerable to the gathering of personal information by surreptitious means, often without the individual's consent.

As global reliance on cyberspace continues to grow, so too does the scope of damage that malicious actors can impose.⁵ Two experts have defined cyberspace as “a complex of electronic networks that cross state and national boundaries. Since cyberspace recognises no geographic boundaries, its full social, political, and economic potential has yet to be realised. The advent of such a radically new phenomenon tests the adaptability of the legal system.”⁶ This is no surprise given that the cybercrime legislative vacuum has often been addressed in a stopgap manner. Such a climate of *ad hoc* legislative thinking inevitably led to a patchwork of global computer crime provisions reflecting incongruent governmental interests.⁷

A noticeable feature of the information technology revolution is the impact it has had and will continue to have on the evolution of telecommunications technology. This revolution in information technologies “has changed society fundamentally and will probably continue to do so in the foreseeable future.”⁸ Information technology has, in one way or another, pervaded almost every aspect of human activity. Nearly wholesale reliance on computers is not only a significant vulnerability, but it also operates as an ideal target for exploitation. Cybercrime has gladly embraced the borderless and anonymous characteristics of the Internet and, by so doing, presents a significant and demanding challenge to international legislatures. Consequently, in light of this new and international dimension of computer crime, governments have

⁵ Olsen, “The Threat of Systematic and Organised Cybercrime and Information Warfare,” available at <http://www.lib.umi.com>.

⁶ Gilligan & Imwinkelried, “Cyberspace: The Newest Challenge for Traditional Legal Doctrine,” 24 *Rutgers Computer and Technology Law Journal* 305 (1998).

⁷ O’Herlihy, “The Cybercrime Convention: A Pioneering Text of International Legal Scope?” [2003] *Hibernian Law Journal* 145 at 146.

⁸ European Committee on Crime Problems, “Final Activity Report 2001,” available at <http://www.privacyinternational.org/issues/cybercrime/coe/cybercrimememo-final.html>.

recognised the need of ensuring that legal protection is harmonised among nations. The Cybercrime Convention⁹ represents the very first international attempt to legislate in this area. However, as this paper will go on to illustrate, pulling in the opposite direction of the treaty is a strong national preference for individualistic rights, such as private property, political freedom and privacy: a preference entrenched in written constitutions containing entrenched Bills of Rights, administered by largely activist judiciaries.

II. COMPUTERS AS CRIMINALS

The word “cybercrime” does not appear in most dictionaries, (including Microsoft’s online Encarta), but that does not mean that the phenomenon doesn’t exist. It is primarily due to the relative newness of this phenomenon that it is difficult to illustrate the earliest incidences of computer crime. Broadly speaking, the term can be defined as a subcategory of computer crime, i.e. the term concerns the criminal offences committed using the Internet or another computer network as a component of the crime.¹⁰

But what is clear is that society, historically, has always, in one form or another, tried to use new forms of technology for personal gain or sabotage. Cybercrime “spans not only state but national boundaries as well.”¹¹ As detractors have rightly pointed out, there is no universally recognised or accepted definition of computer crime. Broadly speaking, however, if an illegal action is committed by the utilisation of information communication technology (ICT), the act is deemed to fall into the category of cybercrime. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues

⁹ The Convention on Cybercrime is available at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

¹⁰ Shinder, *Scene of the CyberCrime Computer Forensics Handbook* (Rockland, MA, 2002), p. 5.

¹¹ *Ibid.* at p. 17.

of crimes related to computer networks, cybercrime was broken into two categories and defined as:

A. Cybercrime in a narrow sense (computer crime):

Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them.

B. Cybercrime in a broader sense (computer-related crime): Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.¹²

Such a definition is complicated by the fact that an act may be illegal in a certain nation, but not in another. Therefore, it should not be seen as all-encompassing, rather an international guiding principle on what is an amorphous concept. In order to comprehend the nature of computer crime, one must first be familiar with the players. While no classification system exists for cybercriminals, several categorisations of hackers are widely accepted.¹³ The term hacker is applied to a variety of individuals who are adept at manipulating technology. Hackers use their skills to gain unauthorised access to any electronic system. Skill levels aside, according to their intent and motivation, hackers may be subdivided into three broad categories: white hats, black hats and developers. Of great concern is that the motivations and varieties of hackers have diversified and they have developed an extensive subculture as pointed out by Paul Taylor:

Western Society has an ambivalent relationship with rapid technological change. On one hand western society has a vested interest in believing that maverick tendencies distinguish it from the most regimental and unimaginative oriental culture, yet, on the otherhand, it seeks to control and punish such creativity when it is

¹² *Ibid.* at p. 17.

¹³ Taylor, *Hackers: Crime in the Digital Sublime* (London, 1999).

perceived to have overstepped its boundaries and gone beyond its control.¹⁴

Another problematic development is the prevalence of hacker training courses and schools throughout the world. The computer intrusion tools employed by the hackers are becoming increasingly available on the Internet, while the attack potential of software has become more sophisticated with an increased ability of causing damage.¹⁵ This is a very worrying trend considering that the number of personal computer owners and users that possess Internet capabilities continually increases. This is especially evident in the United States, which has the “world’s most technologically vulnerable nation.”¹⁶ Moreover, in February 2002, Nua Internet Surveys showed that approximately 544 million people were online worldwide. Consequently, as the global population becomes ever more “connected,” the level of opportunity for criminals to use the Internet to violate the law will expand and cybercrime will touch more and more lives.¹⁷ It is suggested that “by 2005 some sixty one percent of Europeans and sixty four percent of Americans will have access to the Net on PC.”¹⁸

Since the Internet offers a range of lucrative opportunities, organised crime is ideally suited to profit from the information revolution. Moreover, so long as the Internet continues to serve as a safe haven for illicit activities,¹⁹ cybercriminals will continue to operate with little or no risk of being identified or facing judicial prosecution. Since operations of an illicit nature regularly cross geographical

¹⁴ *Ibid.* at p. 170.

¹⁵ Congress, Senate, Committee on Judiciary, Subcommittee for Technology, Terrorism and Government Information Cybercrime. Congress statement is available at <http://www.usdoj.gov/criminal/cybercrime/freeh328.htm>. (last accessed 10 January 2005).

¹⁶ Nielsen/Netratings Global Internet Trends is available at <http://www.nielsenmedia.com>. (last accessed 8 January 2005).

¹⁷ Shinder, *Scene of the CyberCrime Computer Forensics Handbook* at p. 10.

¹⁸ Cronin, “An analysis of the Irish Data Protection Law in relation to the protection of privacy in the online environment” [2003] *Cork Online Law Review* at *5.

¹⁹ White House Press Release available at: <http://www.state.gov/p/eur/rls/prsr/2003/26308.htm>. (last accessed 8 December 2004).

boundaries and state borders, national law enforcement agencies are frequently unable to pursue international cybercriminals.²⁰ In light of this international dimension of computer crime, governments have recognised the need of ensuring that legal protection is harmonised among nations.

III. BACKGROUND TO THE CONVENTION ON CYBERCRIME

“By necessity, the fight against cybercrime must involve more than just the police. Legislators must make appropriate laws.”²¹

In recent years, certain international bodies, such as the Council of Europe, the Organisation for Economic Co-operation and Development (OECD), or the G8 Conference, have begun to consider issues pertinent to the area of cybercrime as part of their policy agenda.²² As observed by Ian Walden, numerous attempts have been undertaken within several international organisations and *fora*, such as the G8 Member States, (e.g., the G8 Recommendation on Transnational Crime), to achieve a harmonised approach to legislating against computer crime and thereby try to prevent the appearance of “computer crime havens.”²³ The first such major attempt was under the guidance of the OECD. However, the most significant institution in the field has been the Council of Europe (COE). The Council first analysed the problems associated with the international nature of cybercrimes when it drafted a 1995 paper recommending that the various states adopt laws concerning cybercrime. Realising the need for a legally binding instrument, the Council began deliberating on the cybercrime treaty in 1997.²⁴ Despite its admirable objectives, the Convention haplessly progressed through its drafting process in a hostile arena engulfed with

²⁰ Kennedy, “In Search of a Balance between Police Power and Privacy in the Cybercrime Treaty,” 9 *Richmond Journal of Law & Technology* at *4.

²¹ Shinder, *Scene of the CyberCrime Computer Forensics Handbook* at p. 35.

²² Dr. Paul Norman, “Policing High Tech Crime in the Global Context,” available at <http://www.bileta.ax.uk/99papers/morman.htm>. (last accessed 2 February 2005).

²³ Reed and Angel, *Computer Law* at p. 295.

²⁴ *Ibid.* at p. 296.

confrontation between human rights activists, law enforcers and corporate industry representatives.

It took a staggering gestation period of over four years and twenty-seven drafts for the then forty-two nation COE, coupled with the U.S., Canada, Japan and other countries participating as “observers,” to draft the Cybercrime Convention.²⁵ The treaty is intended to create a common cross-border criminal policy aimed at the protection of society against cybercrime by adopting appropriate legislation and fostering international co-operation.²⁶ In reality, American law enforcement officials have been the primary drivers behind the treaty.

IV. THE FRAMEWORK OF THE CONVENTION

The Convention contains a total of forty-eight Articles comprising four chapters that include: (i) Use of Terms; (ii) Measures to be taken at Domestic Level – Substantive Law and Procedural Law; (iii) International Co-operation; and (iv) Final Clauses.²⁷

The Convention has three broad parts. The first proposes that all signatories criminalise certain on-line activities. The second stipulates that states should require the operators of telecommunications networks or Internet service providers (ISPs) to institute more detailed surveillance of network traffic and where possible real-time analysis. And Part Three requires that states cooperate with each other in the investigation of cybercrime by allowing data to be shared among them. This is especially true even if the crime being investigated in one state is not a crime in the state from the information is being requested.

²⁵ O’Herlihy, “The Cybercrime Convention: A Pioneering Text of International Legal Scope?” [2003] *Hibernian Law Journal* at 147.

²⁶ Keyser, “The Council of Europe Convention on Cybercrime,” 12 *Florida State University Journal of Transnational Law and Policy* 287 (2003).

²⁷ The Convention on Cybercrime is available at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>. (last accessed 19 November 2004).

The Convention, therefore, does three major things:

1. It includes a list of crimes that every signatory must have on its books. The treaty requires the criminalisation of offences such as hacking, the production, sale or distribution of hacking tools, and child pornography, and an expansion of criminal liability for intellectual property violations (Articles 2-11).
2. It requires that each participating nation is to award new powers of search and seizure to its law enforcement authorities, including the power to order an ISP to preserve a citizen's internet usage records or other data, including the authority to monitor a citizen's online activities in real time (Articles 16-22).
3. It requires that the existing law enforcement in every participating country is to assist police from other participating countries by cooperating with "mutual assistance requests" from police in participating nations "to the widest extent possible" (Articles 23-35).²⁸

V. THE CASE FOR RATIFICATION: A MYTH OR A REALITY?

The Treaty only required ratification by five countries to come into force.

Croatia, Albania, Estonia, Hungary and Lithuania have already fulfilled this function and, consequently, the convention came into effect on the 1st of July 2005.²⁹

According to Walter Schwimmer, the Secretary General of the Council of Europe:

The Convention on Cybercrime is a ground-breaking agreement which will play a key role in fighting computer related crime. Cybercrime is a major global challenge which requires a coordinated international response – I therefore urge all of those Council of Europe Member States which have not yet signed the convention to do so as a matter of policy.³⁰

²⁸ "Eight Reasons the International Cybercrime Treaty Should Be Rejected," available at <http://www.treatywatch.org/about.html>. (last accessed 17 February 2005).

²⁹ Since then, France, Romania, Denmark, Cyprus, Bulgaria, Slovenia, and the former Yugoslav Republic of Macedonia have ratified the Convention bringing the total number of ratifications to 12.

³⁰ "Walter Schwimmer Approves Draft Convention," available at <http://www.out-law.com/search/searchresults>. (last accessed 4 January 2005).

The President of the United States, George W. Bush, has also spoken of the Treaty in an equally admirable context, calling it “an effective tool in the global effort to combat computer-related crime” and “the only multilateral treaty to address the problems of computer-related crime and electronic evidence gathering.”³¹

Despite the aforementioned words of praise for the treaty and the risks associated with cybercrime, the Convention is not without its critics. For example, many opponents have cited privacy issues, while others have highlighted the forced cooperation clause. Very notable vociferous opponents of the treaty include civil libertarians who have objected to the treaty since it became public in early 2000. They argue that it would endanger privacy rights, as well as allocate too much power to government investigators.

Barry Steinhardt, director of the American Civil Liberties Union (ACLU) technology and liberty program, argues that it is a treaty that will far surpass its intended remit. Before the Senate of the United States, he opined that “it would require nations that participate in the treaty to adopt all sorts of intrusive surveillance measures and cooperate with other nations, even when the act that’s being investigated is not a crime in their home country.”³² This portion of the treaty therefore, requires each country to pass laws that allow governments to search and seize email and computer records, perform Internet surveillance, and to order ISPs (Internet Service Providers) to preserve logs in connection with an investigation. This is known as the “mutual assistance” provision.

Thus, under the treaty, it will be a crime to create, download or to post on a website any computer program designed or adapted with the main aim of gaining access to a computer system without permission. Software designed to interfere with

³¹ “Senate Debates Cybercrime Treaty,” available at <http://ecoustics-cnet.com> , *1. (last accessed 4 January 2005).

³² *Ibid.* at *2.

the functioning of a computer system, either by the deletion or alteration of data, is also prohibited. The treaty will make it permissible for authorities to order an individual to disclose her pass phrase for an encryption key. Leading analysts argue this could be repugnant with the constitutional protections against self-incrimination afforded citizens of the United States. The convention will also require websites and Internet providers to collect information concerning their users, a rule which, it is argued, will potentially limit anonymous retailers.

VI. KEY CRITICISMS OF THE TREATY

The treaty was drafted in a closed and secretive manner. As Kennedy³³ posits, up until the release of the proposed treaty, member delegations had worked in virtual secrecy on the negotiations. This closed, reticent and undemocratic drafting process triggered much anger and was the catalyst for the condemnation by a coalition of international cyber-rights organisations, which represented the views of data protection officials, privacy experts and technical experts. A common complaint from the public-interest groups was they did not have a seat on the negotiations table which, as they argue, was dominated by law enforcement officials.³⁴ What seems to have further enraged the public-interest groups was that, after the subsequent publication of treaty drafts, the authors made little or no effort to incorporate the groups' concerns and views. In a letter to the Council of Europe, Global Internet Liberty Campaign (GILC) stated that this process was devoid of any democratic means of accountability and lacked transparency.³⁵

³³ Kennedy, "In Search of a Balance between Police Power and Privacy in the Cybercrime Treaty," 9 *Richmond Journal of Law & Technology* at *6.

³⁴ O'Herlihy, "The Cybercrime Convention: A Pioneering Text of International Legal Scope?" [2003] *Hibernian Law Journal* at 147.

³⁵ "Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime," available at <http://www.gilc.org/privacy/coe-letter-1000.html>. (last accessed 10 February 2005).

A further criticism of the treaty is that it is too broadly drafted. Its critics argue that the treaty is no longer confined to covering computer-related crimes and instead expands to any crime where the evidence could be in a computerised form (Article 23). A direct consequence of this provision would be that foreign police would be able to order a search to investigate an individual's computer records, thereby infringing on her privacy rights.

Of greater interest in relation to the above criticism is that the word "privacy" is not even mentioned in any of the convention's forty eight articles. In addition, the treaty lacks necessary search and seizure procedural safeguards according to privacy advocates. Kennedy argues that the absence of such search and seizure procedures could allow a "race to the bottom" in relation to the protection of privacy.³⁶ Thus, it is argued that, while the treaty has significantly increased police power, it has neither maintained nor increased guarantees of privacy. Such a lack of a privacy provision is contrary to other international law enforcement agreements, such as Interpol, Europol and Schengen agreements.

Law enforcement officials in one nation can, under the Convention, be obligated to comply with investigations concerning individual(s) acts that may be perfectly legal within their own borders but is illegal in another country. This results from the Convention's lack of a "dual criminality" provision, which would ordinarily require the act to be a crime in both countries before one nation could procure the police of another nation to aid the investigation. This especially worries civil libertarians because the treaty would be open to any country seeking to prosecute individual(s) from other ratifying countries. They argue that some of these mutual assistance requests will come from countries with minimal civil liberties protections.

³⁶ Kennedy, "In Search of a Balance between Police Power and Privacy in the Cybercrime Treaty," 9 *Richmond Journal of Law & Technology* at 13.

A direct consequence of this could be that it would render the surveillance capabilities of the United States at the disposal of foreign governments with poor human rights records.

Crucially, however, there is a clause contained within the treaty that allows a country to refuse to cooperate in an investigation if its “essential interests” are threatened by the request. In theory, this would allow the United States to withdraw from a probe targeting free speech or other actions protected by its Constitution. Moreover, certain political offences are specifically excluded from some types of mutual assistance requests available under the treaty, (although it remains to be seen how this will function in practice).³⁷ Critics, however, have cited these exceptions as being far too limited, arguing that they won’t even apply to many of the most significant requests. The exemption for these very offences regarded as “political” in nature was omitted from the pertinent section requiring real-time data monitoring (Article 33). Furthermore, the critics highlight the absence of any definition on what actually amounts to “political offences.” This is a relevant criticism bearing in mind that a criminal offence in one nation may not be a criminal matter in another.

It is argued that the treaty will have a significant impact in the realm of intellectual property law. The so-called vague intellectual property provisions could greatly increase the scope for criminal liability for intellectual property violations and shift copyright law further away from the public interest. The treaty, its opponents argue, makes copyright violations into extradictable offences. “Intellectual Property law in the U.S. and many other nations is a delicate balance between the rights of intellectual propertyholders and the rights of the public. This treaty openly implies that infringement of copyright is to be criminalised, no mention is given to

³⁷ Kevin Poulsen, “U.S. Defends Cybercrime Treaty,” available at http://theregister.co.uk/2004/04/24us_defends_cybercrime_treaty/print.html. (last accessed 10 February 2005).

counterbalancing rights that, for example, allow copyrighted material to be utilised for ‘parodies, criticism, and scholarly analysis.’³⁸

Under Title 4 of the Convention, Member States are required to have successfully implemented the 1971 Paris Act, the Berne Convention for the Protection of Literary and Artistic Works, the World Trade Organisation agreement (WTO) on the Trade-Related Aspects of Intellectual Property Rights (TRIPS), as well as the World International Property Organisation (WIPO) Copyright Treaty. Therefore, there is a duty and an onus on the signatory states to criminalise any such wilful copyright violations carried out on a commercial scale, and by way of a computer system.³⁹

Additionally, the Convention will give police invasive new surveillance powers. Technologies, such as Carnivore (i.e. the “Internet-tapping” surveillance system used by the FBI), would require signatory nations to authorise the use of such a device. A direct consequence would be that law enforcement agencies could have uninhibited access to ISPs’ entire networks for surveillance.⁴⁰ GILC argues that such a proposal that includes creating new investigative and prosecutorial authority should give great consideration to articles 8 and 10 of the European Convention on Human Rights (ECHR). In their opinion, the drafters did not give sufficient consideration to these issues in the convention. A corollary of this new legislation is that groups like GILC and the ACLU, who mount serious challenges to governments or multinational corporations, could, under the legislative framework, be subject to direct surveillance. Governments, it is argued, could manipulate this new system to monitor, as well as retain, communications data in order to map the activities and membership of

³⁸ “Senate Debates Cybercrime Treaty,” available at <http://ecoustics-cnet.com>, at *4.

³⁹ Transnational Law Associates, LLC, International Law Update, Vol.7, No 12. (last accessed 8 February 2005).

⁴⁰ *Ibid.*

campaign groups. They allege this could have detrimental implications for their continuance and functionality.⁴¹

In relation to the already mentioned privacy concerns, civil libertarians argue that the Justice Department will try to coerce the U.S. Senate to approve the treaty regardless if it violates Americans' privacy rights. "The Council of Europe in this case has just been taken over by the U.S. Justice Department and is only considering law enforcement demands. They're using one more international organisation to launder U.S. policy."⁴² According to one free speech activist, Article 6, titled "Illegal Devices," could be construed as banning commonplace network security tools such as crack and nmap, which are standardly included with the product Linux. A potential consequence is that "companies would be able to criminalise people who reveal security holes about their products."⁴³

Since the cybercrime scene has no physical boundaries, an adept hacker can remain incognito in cyberspace. This bears the consequence that, if law enforcement cannot discover the cybercriminal by the clues left in cyberspace, it can be a very arduous and often impossible task to track the criminal.⁴⁴ However, this creates a conflict because, according to Barry Steinhardt, it will interfere with one's ability to speak anonymously. It will interfere with the ability of hackers (using that term in a favourable light) to test their own security and the security of others. However, according to Solveig Singleton, director of information studies at the libertarian Cato Institute it is not a certainty that anonymous remailers will be imperilled.

VII. THE RIGHT TO PRIVACY

⁴¹ "Specific Issues in Internet Policy and Regulation," available at <http://www.apc.org/english/rights/handbook/ICT22.shtml>. (last accessed 4 February 2005).

⁴² McCullagh, "Cybercrime Solution has Bugs," available at <http://www.wired.com/news/print/0,1294,36047,00.html>. (last accessed 10 February 2005).

⁴³ *Ibid.* at *2.

⁴⁴ Kennedy, "In Search of a Balance between Police Power and Privacy in the Cybercrime Treaty," 9 *Richmond Journal of Law & Technology* at *9.

The third criticism with respect to privacy rights seems to have generated the most vociferous response from critics of the convention. Hence, it deserves some consideration, bearing in mind privacy in an Irish context. Previous rulings from Irish courts indicate that a right to privacy does exist in this jurisdiction, but that the right is not absolute.⁴⁵ Alan Westin, a leading expert on the issue, describes privacy as “the voluntary and temporary withdrawal of a person from the general society through physical or psychological means...”⁴⁶ Notable precedents include *Kennedy v. Ireland*,⁴⁷ where Hamilton, P. explicitly recognised the right to privacy of communications stating that “the dignity and freedom of an individual in a democratic society cannot be ensured if his communications of a private nature are deliberately, consciously and unjustifiably intruded upon and interfered with.” Thus, the right to privacy is not unlimited. For example, Dworkin states that the pressure of those who wish to obtain a right of privacy is often met by other pressures from those who, whilst not unsympathetic to certain kinds of privacy interests, are demanding greater rights to know, to publish and to use private information.⁴⁸

While Data Protection Legislation exists, as does the European Data Protection Directive and Article 40.3.1 of the Irish Constitution, there remains no specific legislation in this jurisdiction that deals with Internet and e-mail privacy. This is a common scenario in most areas of the law where technological innovation has outpaced legislative reform.⁴⁹ Cronin, in his article,⁵⁰ proposes that the easiest method for e-mail users to protect their communications would be to send messages

⁴⁵ *Murray v. Ireland* [1991] I.L.R.M. 465.

⁴⁶ Kennedy, “In Search of a Balance between Police Power and Privacy in the Cybercrime Treaty,” 9 *Richmond Journal of Law & Technology* at *13.

⁴⁷ *Kennedy v. Ireland* [1987] I.R. 553.

⁴⁸ Dworkin, *Privacy and the Law* (John Wiley & Sons, 1978).

⁴⁹ Cronin, “Who’s Minding your Business?: E-Mail Privacy in the Workplace” [2002] *Cork Online Law Review*, available at <http://colr.ucc.ie/2002vi.htm>.

⁵⁰ *Id.* at *4.

anonymously. However, he acknowledges that the threat of such a system is that it could lead to online problems such as harassment and defamation. As noted *supra*, without the fear of ones identity being revealed, a cybercriminal could willingly engage in such practices and the recipient would have no redress. Ordinarily, for those seeking privacy protections of a more secure nature, the introduction of encryption programmes could be considered.

This circulates back to the problems with the Convention. For example, in relation to the anonymity point, law enforcement officials in one nation, can, under the treaty, be obligated to comply with investigations concerning individual(s) behaviour that may be perfectly legal within their own borders, but illegal in another country because of the absence of a “dual criminality” provision. In relation to the encryption point and so called stronger electronic privacy protection, the Convention could make it permissible for authorities to order an individual to disclose his passphrase for an encryption key. Leading analysts argue this could be repugnant to certain constitutional protections, for example, those against self-incrimination afforded citizens in the United States.

VIII. EVALUATION OF THE CONVENTION

Having looked at the Convention in some detail, this paper now examines two the foremost concerns about the Convention: international cooperation and privacy issues. It very briefly considers the other two concerns: jurisdiction and sovereignty. The Convention has been immersed in criticism since its introduction. Regarding privacy, the very clandestine manner in which negotiations over the proposed Convention were conducted immediately led to public outcry on the date of its Internet release. Organisations like GILC highlighted their concerns about the broad provisions of the treaty, especially provisions pertaining to illegal devices.

Information, whether held by consumers, employees, employers or sovereign nations, is an essential and lucrative commodity. Consequently, it must not be ignored or abused. Tragically, however, the treaty drafters have failed to recognise and embrace their obligations to respect an individual nation's privacy. It is even more shocking that a forty-eight Article Convention on CyberCrime, which was supposedly predicated on the assertion that the effective fight against cybercrime required increased, rapid and well-functioning international cooperation in criminal matters, is entirely devoid of the word privacy. Rhetoric about the value of privacy is no longer acceptable. In fact, privacy concerns should be paramount. A Convention deficient of a "dual criminality" provision is not only very worrying for civil libertarians, it could also be seen by nations as a potential source of apathy on the drafters' behalf. This could significantly undermine the Convention and its intentions.

Regarding international cooperation, the Convention currently provides that states are obliged to cooperate with each other to the widest possible extent for the purposes of investigations or proceedings pertaining to criminal offences committed via computer systems and/or data or for the collection of electronic evidence of a criminal offence.⁵¹ Moreover, Article 21 provides for extradition and mutual assistance. To this end, nations are required to assign central authorities to deal with and expedite mutual assistance requests. Of particular concern is the expedited preservation of stored computer data. Denis Kelleher⁵² quite rightly points out that such a request can only be refused if the requested nation believes that compliance with the request would prejudice its sovereignty, security or other essential interests. By virtue of Article 24, this preservation must last at least 40 days. Additionally, a

⁵¹ Article 20.

⁵² Kelleher, "The Council of Europe's Draft Convention on Cyber-Crime" [2000] 1(3) *Technology and Entertainment Law Journal* 14.

nation can require another to search and seize, secure or disclose data stored by means of a computer system located within its territory.

With respect to jurisdiction, the drafters have so far proved unsuccessful in their attempt to address the problems raised by the existence of cyberspace. No nation has jurisdiction over cyberspace and it is reasonable to say that the drafters have made little or no attempt to resolve this predicament. In relation to sovereignty, Kennedy makes the point that it remains to be seen why the drafters have allowed intrusions of sovereignty when the treaty allows for the mutual assistance between states, as well as providing expedited mutual assistance where necessary.⁵³

In short, the Convention makes it all too easy for states to conduct cross border investigations, and this will impact and undermine the sovereignty of nations. The Convention, by its own express language, has unnecessarily created four sets of problems that undermine its future efficacy and have plagued its proposed ratification. Whether justified or not, the ubiquitous nature of the Internet makes it impractical to expect European nations not to collaborate closely in the investigation and prosecution of computer crime. Nations and their citizens will not use systems that they perceive as being lawless and unsafe. Until these issues are resolved or, at the very least, acknowledged by the drafters, the Convention in its current state should not be ratified in Ireland.

IX. CONCLUSION

New technologies continue to challenge existing legal concepts. Therefore, so long as cyber criminals continue to operate in places outside of their own domestic borders, solutions to the problems posed must be addressed by international law, thereby necessitating the adoption of ample international legal instruments.

⁵³ *Ibid.*

Debra Shinder, in her book, makes the point that “as nations cooperate with one another in various endeavours, a global vision of what is considered right and wrong has been established on a variety of subjects.”⁵⁴ This is particularly true as international organisations and political coalitions have frequently engaged in dialogue and pressured many countries to create new laws or revise existing ones to deal with crimes that the majority of the world deems too abhorrent to be allowed exist. The Cybercrime Convention is no different in this regard and, while no single treaty is ever likely to address the full scope of the problems created, certain provisions of the Cybercrime Convention still leave a lot to be desired before Ireland is to ratify it.

It is admittedly clear that simply bemoaning the Convention would be disingenuous and ultimately counterproductive. Therefore, it has not been the intention of this paper to undermine the significance of the Convention and the aims of its innovators. It is clear that, taken together, this Convention and earlier authorities represent a valiant effort to bring nations and the law into line. In fact, criticisms of this uniquely modern Convention mirror those typically made of international agreements. However, further redress of the myriad valid issues raised by both individuals and public interest groups namely and discussed in this essay are neither unrealistic, irrational nor unachievable. In the end, while the Convention is unequivocally well-intentioned, as currently constituted, it leaves much to be desired.

⁵⁴ Shinder, *Scene of the CyberCrime Computer Forensics Handbook* at p. 35.