Information and Communications Technologies (ICTs) are now central to the way we interact, both socially and commercially. Inevitably, some people will use ICTs in the commission or facilitation of crime; so-called ‘cybercrimes’. The interconnected nature of modern technology makes this a global problem, and for decades there has been international awareness of the need for coordinated action. The Council of Europe’s Convention on Cybercrime (‘Convention’) was the first multilateral binding instrument to regulate cybercrime. Having recently passed the 10th anniversary of its coming into force, it is timely to reflect on the Convention’s role in the harmonisation of cybercrime laws and its place amongst other international efforts to combat cybercrime. This article begins with a discussion of the importance of harmonisation in combatting cybercrime. There is then a general overview of the Convention, followed by an analysis of three key aspects of harmonisation — the extent to which it is: (1) comprehensive; (2) protective of rights; and (3) representative. Consideration is then given to the desirability and likelihood of an international convention on cybercrime. Although the Convention remains the most significant instrument in this area, it is now accompanied by a range of international, regional and national initiatives. In an environment where an international agreement may be some way off, the Convention provides an important touchstone against which national efforts may be measured. More broadly, the international focus is appropriately moving toward the more pressing issue of capacity building.

I CYBERCRIME: A GLOBAL CHALLENGE

Although by now a familiar story, the pace of technological change continues to amaze. Information and Communications Technologies (ICTs) are now central to the way we interact, both socially and commercially, with in excess of one trillion web sites\(^1\) providing ready access to an incredibly diverse range of information and services. The social networking site Facebook alone has over 1.3 billion monthly active users,\(^2\) and over 100 hours of video is uploaded to YouTube every minute.\(^3\) The estimated value of United States retail e-commerce

---

*Professor, Faculty of Law, Monash University. This article is based on a presentation given at the 2nd International Serious and Organised Crime Conference, Brisbane, 29–30 July 2013. I am grateful to the anonymous referees for their helpful comments on an earlier draft of this article.


sales for the second quarter of 2014 was US$75 billion. Increasingly, we see the so-called ‘internet of things’, with the number of networked devices already exceeding the global population.

Approximately 2.9 billion people, almost 40 percent of the world’s population, are connected to the Internet. While access is highest in developed countries (78 percent of the population compared to 32 percent in the developing world), the actual number of Internet users in developing countries far outnumbers that in developed countries. The convergence of computing and communication technologies has further accelerated this process, with mobile telephony now accessible to 96 percent of the world’s population.

Inevitably, some will use ICTs in the commission or facilitation of crime; so-called ‘cybercrimes’. These include crimes in which ICTs are the target of the criminal activity, existing offences where ICTs are a tool used to commit the crime, and crimes in which the use of ICTs is incidental but may afford evidence of the crime. The interconnected nature of the technology makes this a global problem, and for decades there has been international awareness of the need for coordinated action.

The product of over 16 years of preparatory work, the Council of Europe’s Convention on Cybercrime was the first multilateral binding instrument to

---

4 Ian Thomas, William Davie and Deanna Weidenhamer, United States Department of Commerce, Quarterly Retail E-Commerce Sales 2nd Quarter 2014 (15 August 2014) United States Census Bureau <http://www2.census.gov/retail/releases/historical/ecomm/14q2.pdf>.
10 United Nations Office on Drugs and Crime, ‘Comprehensive Study on Cybercrime’ (Report, February 2013) 1 (‘Comprehensive Study on Cybercrime’).
12 A number of terms are used synonymously and often interchangeably including ‘computer crime’, ‘high-tech crime’, ‘digital crime’, ‘electronic crime’ and ‘technology-enabled’ crime.
regulate cybercrime. The Convention opened for signature on 23 November 2001 and entered into force on 1 July 2004. Having recently passed the 10th anniversary of its coming into force, it is timely to reflect on the Convention’s role in the harmonisation of cybercrime laws and its place amongst other international efforts to combat cybercrime.

This article begins with a discussion of the importance of harmonisation in combatting cybercrime. There is then a general overview of the Convention, followed by an analysis of three key aspects of harmonisation — the extent to which it is: (1) comprehensive; (2) protective of rights; and (3) representative. Consideration is then given to the desirability and likelihood of an international convention on cybercrime. Although the Convention remains the most significant instrument in this area, it is now accompanied by a range of international, regional and national initiatives. While these initiatives provide an important diversity of views — allowing the tailoring of responses according to national perspectives — the greatest danger is fragmentation of effort. In an environment where an international agreement may be some way off, the Convention provides an important touchstone against which national efforts may be measured. More broadly, the international focus is appropriately moving toward the more pressing issue of capacity building.

II THE IMPORTANCE AND CHALLENGES OF HARMONISATION

It is generally accepted that some degree of harmonisation between countries is vital if effective regulation of cybercrimes is to be achieved. Although many offences are transnational in nature — for instance trafficking in humans, weapons and drugs, money laundering and terrorism — cybercrime presents unique challenges due to the inherently transnational nature of the underlying technology. No other type of crime can become transnational so effortlessly. The Bredolab botnet, for example, was estimated to have infected 30 million computers at its peak, generating 3 billion infected emails per day. At a more fundamental level, the nature of modern communications is such that even where offender and victim are in the same jurisdiction, evidence of the offending is almost certain to have passed through, or to be stored in, other jurisdictions. In a recent United Nations study, over half of responding countries reported that ‘between 50 and 100 per cent of cybercrime acts encountered by police involved a “transnational element”’.  

17 See Part V below.
19 Comprehensive Study on Cybercrime, above n 10, 56.
21 Comprehensive Study on Cybercrime, above n 10, 55.
In broad terms, harmonisation is essential for two reasons. The first is to eliminate or at least reduce the incidence of ‘safe havens’. If conduct is not criminalised in a specific country, persons in that country may act with impunity in committing offences that may affect other jurisdictions. Not only is there no ability to prosecute in the home jurisdiction, efforts at evidence gathering and extradition are likely to be thwarted in the absence of dual criminality. This raises the second and more far-reaching rationale; that harmonisation is crucial for effective cooperation between law enforcement agencies.

Although desirable, harmonisation presents considerable challenges when seeking to address issues as complex and diverse as substantive and procedural law, mutual assistance and extradition. Each country brings its particular perspective, influenced by its legal tradition(s) as well as cultural and historical factors. Even at the national level, there can be issues of harmonisation between state or provincial and federal governments. In the international sphere, harmonisation may be with other countries, regionally or internationally. Although any international response to cybercrime must therefore seek to accommodate and reconcile these differences, it must be emphasised that ‘harmonised’ does not mean ‘identical’. What is required is complementarity — enabling enforcement mechanisms to work effectively while respecting national and regional differences.

As the most ambitious attempt to achieve harmonisation in the field of cybercrime, the Convention provides the ideal vehicle for analysis of some of the specific challenges of achieving harmonisation in this area. These challenges will be analysed under three criteria. First, the extent to which it comprehensively addresses the challenges of cybercrime. Second, the extent to which it protects fundamental rights. Third, the extent to which it is representative of different legal systems. While the focus of this article is on the Convention, these issues are equally applicable to any attempt to achieve international agreement in relation to cybercrime.

**A Comprehensive**

To date, the focus of cybercrime laws around the world has largely been on criminalisation — creating new offences or adapting existing offences to address the challenges of cybercrime. However, this is merely one aspect and from its inception the Convention sought to provide a comprehensive response, addressing issues of substantive offences, procedural laws and international cooperation.

---

22 The three major legal traditions are civil law, common law and Islamic law: United Nations Office on Drugs and Crime, ‘Manual on Mutual Legal Assistance and Extradition’ (United Nations, September 2012) 9 (‘Manual on Mutual Legal Assistance and Extradition’). Some jurisdictions may be described as ‘mixed law’, for example, Chinese law which draws upon a range of legal systems: Comprehensive Study on Cybercrime, above n 10, 57 n 21.

23 Comprehensive Study on Cybercrime, above n 10, 59–60.

24 Ibid 53.

Aside from provisions concerned with ancillary and corporate liability and sanctions, the \textit{Convention} provides for four broad categories of substantive offences: (1) offences against the confidentiality, integrity and availability of computer data and systems; (2) computer-related offences (computer-related fraud and forgery); (3) content-related offences (child pornography); and (4) criminal copyright infringement. While in some respects the \textit{Convention} has proved to be remarkably resilient — capable of adapting to new forms of technology such as botnets; clearly these offences do not encompass the full spectrum of cybercrimes. Notable omissions include identity theft, sexual ‘grooming’ of children, unsolicited emails or ‘spam’ and so-called ‘cyberterrorism’.

Although there is certainly room for improvement, it must be remembered that differences relating to the content of the criminal law often depend on socio-

\begin{itemize}
  \item \textit{Convention} ch II s 1 title 5.
  \item Ibid ch II s 1 title 1.
  \item Ibid ch II s 1 title 2.
  \item Ibid ch II s 1 title 3.
  \item Ibid ch II s 1 title 4.
\end{itemize}
cultural factors; for example, differing attitudes to freedom of expression. Differences may also arise due to varying levels of technical capacity. Spam, for example, is an issue that many developing countries would like to see criminalised, but is addressed by most developed countries as a civil or administrative matter. There is therefore a distinction between offences that were not anticipated, and those on which international agreement could not be reached. While it is possible to incorporate the former within an amended or new convention, the latter will necessarily limit the scope of any convention.

The Convention itself makes provision for the parties to consult periodically to facilitate its ‘effective use and implementation’, the exchange of information and ‘consideration of possible supplementation or amendment of the Convention’. Any party may propose an amendment to the Convention, although whether it is adopted is ultimately a decision of the Committee of Ministers, taking into account the opinion of the European Committee on Crime Problems and consultation with non-member state parties. This mechanism has already been utilised in relation to the Additional Protocol on Acts of a Racist and Xenophobic Nature, and is currently being used as the basis for discussion of an additional protocol in relation to transborder access to data.

Further, the Convention does not preclude other national, regional or international bodies addressing these substantive offences to the extent they are not inconsistent with the Convention. For example, the European Parliament and Council are given power to set minimum rules in relation to definitions and sanctions with respect to ‘computer crime’. It is therefore one mechanism whereby member states may update their cybercrime legislation, even if the Convention remains static.

While globally some attention has been given to substantive offences, less focus has been given to the equally, if not more important areas of investigation, criminal

38 Comprehensive Study on Cybercrime, above n 10, 58.
40 Clough, above n 37, 379.
41 Convention art 46(1).
42 Ibid art 44(3).
44 Transborder Group, ‘(Draft) Elements of an Additional Protocol to the Budapest Convention on Cybercrime Regarding Transborder Access to Data’ (Draft Proposal, Cybercrime Convention Committee, Council of Europe, 9 April 2013). This issue is discussed in more detail below in Part II(B)(4).
47 Gerecke, ‘10 Years Convention on Cybercrime’, above n 37, 144.
procedure, evidence and international cooperation. One of the most striking and challenging features of the Convention is the comprehensive approach it adopts in relation to these broader issues.

1 Investigation

The challenges of digital investigations are addressed in the Convention ch II s 2. Because of the inherent volatility of digital evidence, this includes powers for the expedited preservation of stored computer data, and the expedited preservation and partial disclosure of traffic data. These powers allow for relevant data to be preserved, allowing authorities time to seek its disclosure. Partial disclosure of traffic data is also allowed in order to identify the path through which the communication was transmitted. Provision is also made for production, or search and seizure of data, as well as real time collection of traffic data and/or interception of content data.

These procedures must be applied to those offences provided for under arts 2–11. Further, to help ensure equivalence between the collection of non-digital and digital evidence, and subject to limited exceptions, they must also be applied to other offences committed by means of a computer system, or where evidence is collected in electronic form. This reflects the fact that the importance of electronic evidence extends beyond ‘cybercrimes’ to potentially any form of offending to which electronic evidence may be relevant.

2 International Cooperation

At the domestic level, both substantive offences and investigative powers may be enacted without recourse to international agreement. It is when those offences and procedures are to be applied outside of the jurisdiction that international agreement becomes of crucial significance. The ability to carry out investigations affecting the territory of other states, so-called ‘investigative jurisdiction’, is addressed in ch III of the Convention. The Convention does not expressly provide

48 Comprehensive Study on Cybercrime, above n 10, 53.
49 Convention art 16.
50 Ibid art 17. ‘Traffic data’ is defined in art 1 as ‘any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service’.
51 Ibid art 18.
52 Ibid art 19.
53 Ibid ch 2 s 2 title 5.
54 Convention Explanatory Report, above n 25, [141].
55 Convention art 14(2).
56 Comprehensive Study on Cybercrime, above n 10, 55.
for the principle of reciprocity,57 but does state that parties are to cooperate with each other ‘to the widest extent possible’ in the investigation of cybercrimes and the collection of electronic evidence.58 This includes the sharing of information without request where it would assist another party in its investigation or which it believes might assist the receiving party in the investigation of any offence that could lead to a mutual assistance request under the Convention.59

Of course, not all investigations can be conducted on an informal or voluntary basis, and so provision is made in the Convention for mutual assistance. These provisions mirror the procedural powers discussed above, including expedited preservation of stored computer data and expedited disclosure of traffic data.60

In the case of real time collection of traffic data and interception of content data, parties shall give such assistance as permitted under their domestic laws and applicable treaties (subject to reservations to the Convention’s provisions).61

Consistently with the general principle in art 23, parties are also to afford mutual assistance ‘to the widest extent possible’ in respect of ‘offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence’.62 As with voluntary cooperation, this latter point recognises that effective international cooperation is important not just for ‘cybercrimes’ in the narrow sense, but for all offences involving digital evidence.63

Parties may, however, restrict their level of cooperation more narrowly in cases of extradition, mutual assistance regarding the real time collection of traffic data and mutual assistance regarding the interception of content data.64 More broadly, this general principle of cooperation is to be carried out ‘through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws’.65 This reinforces the general principle that cooperation under ch III does not supersede these other instruments and arrangements.66

In order to facilitate cooperation, both formal and informal, the Convention also provides for a 24/7 network to be created, whereby each party designates a contact point, to be available at all times, to provide immediate assistance for the purpose of cybercrime investigations or proceedings or the collection of

57 In contrast, the United Nations Convention against Transnational Organized Crime, opened for signature 12 December 2000, 2225 UNTS 209 (entered into force 29 September 2003) art 18(1) (‘UNTOC’) states that parties ‘shall reciprocally extend to one another similar assistance’ where there are reasonable grounds to suspect that the offence is transnational in nature.
58 Convention art 23.
60 Ibid arts 29–30.
62 Ibid art 25(1).
63 Convention Explanatory Report, above n 25, [243], [253].
64 See Part II(B) below.
65 Convention art 23.
66 Convention Explanatory Report, above n 25, [244].
electronic evidence.\textsuperscript{67} This provision is based on the experience of the G8 network of contact points, which currently consists of 50 members.\textsuperscript{68}

If implemented, one of the most significant changes to result from the \textit{Convention} would be the expedited processing of urgent mutual assistance requests. Current mutual assistance mechanisms are notoriously slow, and may take months as they pass through bureaucratic channels using traditional means.\textsuperscript{69} The \textit{Convention} makes provision for parties, in ‘urgent circumstances’, to make mutual assistance requests and communications using ‘expedited means of communication, including fax or e-mail’.\textsuperscript{70} Such means need only be utilised to the extent that they provide appropriate levels of security and authentication.\textsuperscript{71} The requested party must accept and respond to the request using expedited means of communication, with formal confirmation only necessary if at the request of the requested party.\textsuperscript{72}

### 3 Jurisdiction

In terms of substantive jurisdiction, that is, the ability of states to assert jurisdiction over criminal offences,\textsuperscript{73} the \textit{Convention} requires parties to establish jurisdiction over the offences established under arts 2–11 when they are committed within its territory, on board a ship or aircraft flagged or registered under the laws of that party, or by one of its nationals if the offence is punishable under the criminal law where it was committed, or if the offence is committed outside the territorial jurisdiction of any state.\textsuperscript{74}

While the goal is to provide as expansive an application as possible, parties may reserve the right not to apply, or to limit the application of, any of the jurisdictional bases other than territoriality.\textsuperscript{75} The \textit{Convention} does not, however, exclude any criminal jurisdiction exercised by a country under its domestic law.\textsuperscript{76} Where more than one party claims jurisdiction, they are to ‘consult with a view to determining

\textsuperscript{67} \textit{Convention} art 35.
\textsuperscript{68} Council of Europe, \textit{Action against Economic Crime: About 24/7 Points of Contact} <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/points%20of%20contact/aboutpocz-EN.asp>. See also the Interpol I-24/7 Secure Global Police Network: Interpol, \textit{Data Exchange} <http://www.interpol.int/INTERPOL-expertise/Data-exchange/I-24-7>.
\textsuperscript{69} \textit{Convention} art 25(3). These are of course illustrative examples, which will develop as technology develops: ibid [256]. For example, Voice over Internet Protocol (VoIP) could be used as a form of communication for these purposes.
\textsuperscript{70} Ibid.
\textsuperscript{71} \textit{Convention Explanatory Report}, above n 25, [256].
\textsuperscript{72} \textit{Convention} art 25(3). These are of course illustrative examples, which will develop as technology develops: ibid [256]. For example, Voice over Internet Protocol (VoIP) could be used as a form of communication for these purposes.
\textsuperscript{73} \textit{Convention Explanatory Report}, above n 25, [256].
\textsuperscript{74} Ibid.
\textsuperscript{75} \textit{Comprehensive Study on Cybercrime}, above n 10, 55.
\textsuperscript{76} \textit{Convention} art 22(1).
\textsuperscript{77} Ibid art 22(2). In total, six countries have exercised this right, albeit to varying degrees — Australia, Belgium, France, Japan, the United Kingdom and the United States: see Council of Europe, \textit{List of Declarations Made with Respect to Treaty No 185} <http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=8&DF=&CL=ENG&VL=1>.
\textsuperscript{78} \textit{Convention} art 22(4).
the most appropriate jurisdiction’. The *Convention* may, however, be criticised for not providing any criteria for the settlement of such disputes. 

### 4 Extradition

The fact that a country asserts jurisdiction over an offence does not automatically translate into the ability to enforce that jurisdiction. As a general principle, at least in common law countries, serious criminal offences will not be tried in absentia. Nor will countries enforce the public law judgments of another state. Therefore the practical ability to prosecute falls to the country that has the defendant in custody. Yet that country may have no interest in prosecuting, or may have one of a number of competing claims to prosecution.

Extradition involves the formal surrender of a person by one state for the purposes of prosecution or for the imposition or enforcement of a sentence in another, and is commonly supported by bilateral treaties. A common requirement of extradition is ‘dual criminality’; that is, in order to be extraditable the offence must be an offence under the laws of both jurisdictions, usually subject to a minimum level of penalty. This causes particular challenges in the context of cybercrime where one jurisdiction may not recognise the relevant conduct as an offence at all. Difficulties may also arise where the relevant extradition treaty adopts an enumerative rather than a prescriptive formulation. The listed offences might not incorporate newer forms of offence, and it is now more common for extradition treaties to define extraditable offences by reference to minimum penalty level, regardless of whether they are classified in the same way.

The *Convention* may play an important role in addressing these issues without the need for renegotiation of individual treaties. Under art 24 each of the offences established under arts 2–11 are deemed to be extraditable offences in any extradition treaty between or among the parties. Parties also ‘undertake to

---

77 Ibid art 22(5).
78 Henrik W K Kaspersen, ‘Cybercrime and Internet Jurisdiction’ (Discussion Paper (draft), Council of Europe, Project on Cybercrime, 5 March 2009) 20–2 [59]–[67].
include such offences … [under] any extradition treaty … concluded between or among them’. 87 Where parties require a treaty as a precondition of extradition but none is in existence, the Convention may provide the necessary legal basis for extradition. 88 Those parties which do not require a treaty for the purposes of extradition are to recognise these offences as extraditable offences. 89

The purpose of this summary has been to illustrate the potentially broad range of powers and obligations under the Convention. Although undoubtedly making it the most comprehensive instrument in this area, 90 they also give rise to some of the most strident criticisms of the Convention and impediments to its wider adoption. This article will now turn to consider some of the most significant objections to the Convention, particularly regarding its approach to protection of individual and state rights.

B Protective

The goal of harmonisation, particularly across such a broad spectrum of laws, will inevitably come into conflict with differences in national principles, whether legal or cultural. 91 This is most apparent in the protection of individual rights, where the tension between the need to improve law enforcement capabilities whilst protecting individual freedoms and privacy has been recognised for some time. 92 Recent revelations concerning ‘almost-Orwellian’ government programs for the bulk collection of metadata have dramatically underscored the need to ensure due process and effective rights protection in the digital environment. 93 This has recently prompted the United Nations to state that it is ‘[d]eeply concerned at the negative impact that surveillance and/or interception of communications … as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights’. 94

Given that it applies to many different legal systems and cultures, the approach adopted by the Convention is the pragmatic one of requiring parties to draw upon their own standards under international and domestic law in enacting the necessary protections and safeguards. 95 First, each party is to ‘ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for

87 Convention art 24(2).
88 Ibid art 24(3).
89 Ibid art 24(4).
90 Proposal on Attacks against Information Systems, above n 45, 3.
91 Comprehensive Study on Cybercrime, above n 10, 58.
92 Combating Criminal Misuse No 1, UN Doc A/RES/55/63; Combating Criminal Misuse No 2, UN Doc A/RES/56/121.
93 Klayman v Obama, 957 F Supp 2d 1, 33 (D DC, 2013).
95 Convention Explanatory Report, above n 25, [145].
under its domestic law, which shall provide for the adequate protection of human rights and liberties. These include rights arising under the Convention for the Protection of Human Rights and Fundamental Freedoms and the International Covenant on Civil and Political Rights, as well as ‘other applicable international human rights instruments’. The ICCPR for example, states that ‘[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation’ and that ‘[e]veryone has the right to the protection of the law against such interference or attacks’. Parties must also incorporate the principle of proportionality.

Second, those conditions and safeguards shall include, ‘as appropriate in view of the nature of the procedure or power concerned … judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure’. Finally, ‘[t]o the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties’.

Such an approach has been described as ‘flexible harmonization’, that is, ‘a model of uniform rule making confined to establishing parameters for acceptable substantive rules, leaving the formulation of procedural due process rules to the cultural peculiarities of each nation’. It is presumed that parties to the Convention ‘form a community of trust and that certain rule of law and human rights principles are respected’. While this may facilitate achieving law enforcement goals, it is arguably at the expense of due process and the protection of individual rights, with drafting of these provisions dominated by law enforcement. Beyond aspirational statements it provides for no specific minimum standards of due process, arguably placing too much responsibility on domestic law to provide appropriate protection. In the United States, for example, Fourth

96 Convention art 15(1).
97 Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953) (‘ECHR’).
98 International Covenant on Civil and Political Rights, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) (‘ICCPR’).
99 Convention art 15(1).
100 ICCPR art 17.
101 Convention art 15(1).
102 Ibid art 15(2).
103 Ibid art 15(3).
105 Miquelon-Weismann, above n 14, 354.
107 Miquelon-Weismann, above n 14, 354.
108 Brenner, above n 32, 216.
109 Miquelon-Weismann, above n 14, 341.
Amendment protection against unreasonable search and seizure may not apply to extraterritorial investigations, nor to the investigation of cybercrimes committed by aliens.\textsuperscript{111}

However, such an approach is not unique to the Convention. The ‘decentralized nature of international law, relegating enforcement to domestic legislation, results from the decentralized structure of international society and the inability to enforce violations of binding legal rules’.\textsuperscript{112} Article 58 of the Geneva Declaration of Principles, for example, provides that the ‘use of ICTs and content creation should respect human rights and fundamental freedoms of others, including personal privacy, and the right to freedom of thought, conscience, and religion in conformity with relevant international instruments’.\textsuperscript{113} This approach allows countries to pursue common goals while respecting legitimate national differences, using international human rights law as an ‘important external reference point’.\textsuperscript{114} It is for ‘[n]ational legislatures … to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of particular conditions and safeguards’.\textsuperscript{115}

For example, art 19(4) of the Convention requires each party ‘to empower its competent authorities to order any person who has knowledge about the functioning of a computer system or measure applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking’ of the search and seizure under art 19. Such provisions may require a person to disclose passwords and may contravene the privilege against self-incrimination.\textsuperscript{116} However, this provision is subject to art 15 and so the United States, for example, would be entitled to limit the provision so as not to offend the Fifth Amendment\textsuperscript{117} as this is a condition and safeguard provided for under its domestic law.\textsuperscript{118} In contrast, Australia — which has no constitutional protection of the right against self-incrimination — has provisions to compel password disclosure that apply beyond persons who might incriminate themselves to include suspects.\textsuperscript{119}

\begin{footnotes}
\textsuperscript{111} Miquelon-Weismann, above n 14, 358.
\textsuperscript{112} Ibid 359.
\textsuperscript{114} Comprehensive Study on Cybercrime, above n 10, xii.
\textsuperscript{115} Convention Explanatory Report, above n 25, [147].
\textsuperscript{116} Brenner, above n 32, 216.
\textsuperscript{117} United States Constitution amend V.
\textsuperscript{118} Convention art 15(1). As to the compelled production of passwords and the Fifth Amendment, see United States v Fricosu 841 F Supp 2d 1232 (D Colo, 2012).
\textsuperscript{119} Crimes Act 1914 (Cth) s 3LA. For a comparison of art 15 as applied in the Netherlands and the United States, see Henrik Kaspersen, Joseph Schwerha and Drazen Dragicevic, ‘Article 15: Conditions and Safeguards under the Budapest Convention on Cybercrime’ (Discussion Paper, European Union and Council of Europe, 29 March 2012).
\end{footnotes}
Although it may be argued that ‘the need to eradicate cybercrime cannot outweigh the equally important need to achieve a consensus on minimal standards for securing fundamental procedural due process guarantees’,120 it is unrealistic to expect the Convention to achieve what has not been achieved elsewhere. For example, some have advocated that the Convention should incorporate the highest standards of data protection such as those found in Europe, as opposed to the lower standards applied in countries such as the United States.121 However, it is highly unlikely that international agreement on the nature and scope of those protections could be achieved, with the two main participants in the drafting of the Convention — Europe and the United States — taking widely divergent views on the issue of privacy protection.122 The Convention does not, however, prevent parties from accepting other international standards that are not inconsistent. For example, the Council of Europe’s Data Protection Convention is open to non-member states.123

The alternative of an additional Protocol to the Convention, specifying minimal procedural protections, does not address the underlying problem if it applies only to a limited number of countries and/or is subject to reservations by countries. The Charter of Fundamental Rights of the European Union,124 which might provide a suitable model,125 is a salient example. The Charter enshrines a number of civil and political rights including the right to a fair trial, presumption of innocence, principles of legality and proportionality and protections against double punishment. Although incorporated in the Treaty of Lisbon,126 it affects only the application of European law.127 Further, both the United Kingdom and Poland secured Protocols to the Charter limiting its application in domestic courts.128 The limited and still controversial application of rights, within the relatively homogenous European Union, is an indication of the formidable obstacles that would be faced in trying to achieve consensus on issues as divisive as privacy and due process. This would likely doom any international agreement and would leave international cooperation to be negotiated at the national level.

120 Miquelon-Weismann, above n 14, 360.
121 Brenner, above n 32, 215.
125 Miquelon-Weismann, above n 14, 360.
127 Charter art 51.
Against this background, it is useful briefly to review some of the specific protective mechanisms that the Convention puts in place in order to balance these competing concerns.

1 Investigative Powers

The ‘traditional veil of privacy’ surrounding personal communications has long been subject to exceptions whereby law enforcement may intercept mail, telecommunications, phone records or employ other forms of surveillance. However, the sheer scale of communications data now being generated has the potential to give law enforcement agencies unprecedented access to personal information unless privacy protections are adapted to the modern communications environment. While it may be argued that such access should be granted ‘only in the rarest and most serious of circumstances, subject always to judicial review’, if digital information is to be subject to greater protection than existing communications, it should be through a considered application of privacy laws. Digital communications should not be granted de facto protection simply because the law has failed to keep pace with technology. What the Convention seeks to achieve is an equivalence of laws applying to the digital environment, allowing law enforcement to employ similar techniques to those already employed in relation to other forms of communication.

A possible concern is that the Convention does not express any limitation on the seriousness of those offences that are subject to these investigative powers. Theoretically, they may apply equally to serious or relatively minor offences. Such concerns must, in general, be addressed by the principle of proportionality. That is, it is for individual parties to determine whether particular conduct is sufficiently serious to warrant the application of certain investigative powers, and the circumstances in which those powers may be exercised. However, a specific limitation applies in relation to the interception of content data in recognition of the high level of privacy protection that many states afford to the contents of communications. Accordingly, the power to intercept content data is to be applied to ‘a range of serious offences to be determined by domestic law’.

A related but optional limitation is provided for in relation to the real-time interception of traffic data whereby a party may reserve the right to apply this provision only to certain offences or categories of offence. This recognises that some parties may regard interception of traffic data to be as intrusive as the

129 Huey and Rosenberg, above n 110, 599.
130 Ibid 603.
131 Convention art 15(1). Each power is specified to be subject to arts 14 and 15: at arts 16(4), 17(2), 18(2), 19(5), 20(4), 21(4).
132 Convention Explanatory Report, above n 25, [142].
133 Convention art 21(1) (emphasis added). Under art 21, what is a ‘serious offence’ is to be determined according to domestic law.
134 Ibid art 20.
135 Ibid 14(3)(a).
interception of content data.\textsuperscript{136} This is particularly significant as the distinction between content and traffic data becomes blurred.\textsuperscript{137}

However, the restriction must not be greater than the range of offences to which the party applies the power to intercept content data under art 21. That is, the reservation under art 20 must be as or less restrictive than the range of serious offences to which art 20 applies. Given the potential importance of real-time interception of traffic data in tracing the path of communications, parties that exercise this reservation are invited to do so in a way that allows for the broadest exercise of this power.\textsuperscript{138}

Considerable concern has been raised in relation to the implementation of broad based data retention schemes in order to facilitate access by law enforcement to telecommunications data.\textsuperscript{139} However, while the preservation of data is provided for under art 16, this requires parties to ensure that their competent authorities can order or similarly obtain ‘the expeditious preservation of specified computer data’.\textsuperscript{140} If this obligation is given effect to by means of a preservation order, the party must adopt the necessary measures to require a specified person to preserve and maintain the integrity of the data for up to 90 days. During this time the relevant authorities may seek its disclosure, subject to the possibility of renewal.\textsuperscript{141} It is left to individual countries to specify the precise computer data to be preserved, although it must include ‘traffic data’.\textsuperscript{142}

Importantly, the ‘specified computer data’ that must be preserved is data that has already been stored. That is, the Convention requires mechanisms for data preservation, not data retention,\textsuperscript{143} with the obligations applying only to data that is already in existence.\textsuperscript{144} These obligations are therefore dependent upon what ISPs and other service providers decide or are otherwise required to store. While a broad-based data retention regime would make compliance with such orders much easier, it is not required by the Convention.

\textsuperscript{136} Convention Explanatory Report, above n 25, [143].
\textsuperscript{138} Convention Explanatory Report, above n 25, [143].
\textsuperscript{140} Convention art 16(1).
\textsuperscript{141} Ibid art 16(2). Such orders may also be subject to a confidentiality undertaking: at art 16(3).
\textsuperscript{142} Ibid art 16(1). ‘Traffic data’ is defined in art 1(d); see above n 50.
\textsuperscript{143} Convention Explanatory Report, above n 25, [152].
\textsuperscript{144} Ibid [150].
2 Mutual Assistance

Although parties are to cooperate ‘to the widest extent possible’, there is no obligation to provide information spontaneously, and any provision of information is subject to the domestic law of the providing party. Further, such information may be provided subject to binding conditions, for example, confidentiality. This is particularly important where the provision of information may disclose operational information such as technical capability or techniques, or the subject of ongoing investigations. However, it is the incorporation of both mutual assistance and extradition provisions that may raise concerns as to the extent to which local law enforcement will be required to act at the behest of foreign law enforcement agencies.

The Convention does not, in general, impose mutual assistance obligations on parties. Unless specifically stated to the contrary, mutual assistance is subject to the domestic laws of the requested party or applicable mutual assistance treaties, including the grounds on which the requested party may refuse cooperation. This allows parties to provide appropriate safeguards in respect of people located within their jurisdiction. This is, however, subject to the qualification ‘[e]xcept as otherwise specifically provided’. For example, in relation to offences under arts 2–11 of the Convention, mutual assistance is not to be refused solely on the ground that the request concerns an offence that the requested party considers to be a ‘fiscal offence’. This ‘reflects the growing concern that offences with fiscal overtones, such as money-laundering, are major components of transnational organized crime and should therefore not be immune to investigation, extradition and prosecution’.

Applying the principle of subsidiarity, the Convention may also supplement other multilateral or bilateral agreements between states, or may be utilised where no such agreements are in place. For example, it has been used in tandem with the United Nations Convention against Transnational Organised Crime (‘UNTOC’), as well as bilateral extradition treaties. These agreements must not, however,

---

145 Convention arts 23, 25.
146 Ibid art 26(2).
147 Convention Explanatory Report, above n 25, [261].
148 Convention art 25(4); ibid [254]. A similar approach is adopted in the UNTOC: see Manual on Mutual Legal Assistance and Extradition, above n 22, 22.
149 Convention Explanatory Report, above n 25, [257]. In some jurisdictions, mutual assistance and extradition may be granted under domestic law without reliance on a treaty: see Manual on Mutual Legal Assistance and Extradition, above n 22, 22 [53].
150 Convention art 25(4).
151 Ibid. Although not defined in the Convention, these have been defined in other instruments as ‘offences in connection with taxes, duties, customs and exchange’: European Convention on Extradition art 5.
152 Transborder Access and Jurisdiction Discussion Paper, above n 15, 18 [84].
conflict with the principles of the *Convention*.\(^{155}\) If such measures are not in place, or existing measures do not contain appropriate provisions, parties are required to adopt such legislative measures as necessary to carry out their obligations.\(^{156}\)

Where dual criminality is a condition of mutual assistance under the law or obligations of the requested party, and this is permitted under the *Convention*, this condition is taken to be fulfilled ‘irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party’.\(^{157}\) This does not impose dual criminality in cases where the conduct is not an offence in both countries. Rather, as with extradition,\(^{158}\) it ensures that mutual assistance requests are not defeated due to differences in classification rather than substantive objections.\(^{159}\) For example, while some jurisdictions address the misuse of identity information by specific ‘identity theft’ provisions, the majority continue to rely on a combination of existing fraud and related offences.\(^{160}\) So long as the conduct is criminalised in both countries, then dual criminality will be taken to be fulfilled regardless of how it is classified.

In the event that there is no mutual assistance treaty or arrangement between the parties, art 27 of the *Convention* sets out the basis on which mutual assistance requests will be dealt with.\(^{161}\) Significantly, parties may refuse assistance if the request concerns an offence that the requested party considers to be a political offence,\(^{162}\) or it considers the request ‘is likely to prejudice its sovereignty, security, *ordre public* or other essential interests’.\(^{163}\) It may also postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.\(^{164}\)

Specific provision is made in relation to certain forms of mutual assistance request.\(^{165}\) A party may submit a request for the expeditious preservation of stored data where the requesting party intends to submit a request for mutual assistance for access to that data.\(^{166}\) Preservation must be for at least 60 days in order to allow the requesting party time to submit a request for access to the

---

\(^{155}\) *Convention* arts 23, 39.

\(^{156}\) Ibid art 25(2). In some cases, it may be sufficient for a party to treat the provisions of the *Convention* as self-executing, or existing mutual assistance arrangements may be sufficiently flexible to accommodate the provisions of the *Convention*. See *Convention Explanatory Report*, above n 25, [255].

\(^{157}\) *Convention* art 25(5).

\(^{158}\) See Part II(B)(3) below.

\(^{159}\) *Convention Explanatory Report*, above n 25, [259].


\(^{161}\) These provisions may also apply in whole or in part where such agreements or arrangements are in existence, but only by agreement of the parties concerned. See *Convention* art 27(1). See also *Convention* art 28, which makes provisions for confidentiality and limitation on use in such circumstances.

\(^{162}\) Ibid art 27(4)(a).

\(^{163}\) Ibid art 27(4)(b).

\(^{164}\) Ibid art 27(5).

\(^{165}\) Ibid ch III s 2 title 1.

\(^{166}\) Ibid art 29(1).
Once such a request is received, the data must continue to be preserved pending a decision on that request. Where the preservation request relates to traffic data and the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. Such a request may only be refused on the basis that the request relates to a political offence, or would otherwise ‘prejudice its sovereignty, security, ordre public or other essential interests’.

Although dual criminality is not a condition of providing such preservation, a party that requires dual criminality as a condition for responding to mutual assistance requests may reserve the right to refuse on that basis if it has reason to believe that the condition of dual criminality will not be satisfied at the time of disclosure. This limitation does not apply to offences established under arts 2–11, as parties must have created such offences under their domestic laws. In all cases, a preservation request may be refused on the basis that the request concerns a political offence, or would otherwise ‘prejudice its sovereignty, security, ordre public or other essential interests’.

As these articles expressly state the only grounds on which requests are to be refused, they operate to the exclusion of any existing mutual assistance treaties or arrangements. However, as the nature of the requests becomes more intrusive, greater deference is given to existing arrangements and/or domestic laws. For example, art 30, which relates to mutual assistance regarding the accessing of stored computer data, makes no provision in respect of grounds of refusal. Such grounds would therefore be found in existing treaties or under art 27. Article 33, which relates to mutual assistance in the real-time collection of traffic data, is specifically stated to be governed by the conditions and procedures provided for under domestic laws. The most intrusive form of request, the interception of content data, is completely governed by ‘applicable treaties and domestic laws’.

3 **Extradition**

Concern may be expressed that the *Convention* will expand the extradition obligation of parties to countries with which they would not otherwise enter into extradition arrangements. However, the requirements under the *Convention* are associated with existing or proposed extradition arrangements. All that is required is that the offences created under the *Convention* are designated as extraditable

167 Ibid art 29(7).
168 Ibid.
169 Ibid art 30(1).
170 Ibid art 30(2).
171 Ibid art 29(3).
172 Ibid art 29(4).
173 Ibid art 29(5).
174 Ibid art 25(4).
175 Ibid art 34.
offences; it does not guarantee that extradition will occur. When the Convention itself may be used by a party to support extradition, it is not obligated to do so.\(^ {176}\) In addition, a number of requirements are imposed.

First, these offences will only be extraditable if punishable under the laws of both parties by a maximum penalty of one year imprisonment or more.\(^ {177}\) Therefore, even where an offence would ordinarily be extraditable under the Convention, if it is subject to less than the minimum penalty it is no longer so. For example, a party may impose less than 12 months maximum on the offence of unauthorised access with no aggravating factors. Such an offence would therefore not be extraditable under the Convention.\(^ {178}\) In addition, where the parties have agreed a different (higher or lower) minimum level of penalty for these purposes, then that minimum will apply.\(^ {179}\) For example, in some countries the penalties attached to illegal access offences can range from as low as a fine only or less than six months imprisonment, up to in excess of three years.\(^ {180}\)

Second, extradition is subject to the laws of the requested party and/or applicable extradition treaties.\(^ {181}\) Therefore the ultimate decision to extradite resides in these arrangements, not the Convention. It is commonly the case that extradition will be refused, for example, where the prosecution is seen to be for a political offence,\(^ {182}\) or where the defendant may be subject to torture.\(^ {183}\) Such restrictions continue to apply. In general, there is also a practical impediment — the complexity and cost of the extradition process ensures that it is typically reserved for serious offences.\(^ {184}\)

The application of existing extradition arrangements may nonetheless result in controversial decisions to extradite. For example, Englishman Gary McKinnon fought his extradition to the United States in respect of his alleged unauthorised access to United States federal computers.\(^ {185}\) However, any controversy lies with the extradition arrangements between those countries, not the Convention itself. The Convention merely ensures the possibility of extradition for these offences; it is up to individual parties to determine whether extradition will be granted.

\(^ {176}\) Convention Explanatory Report, above n 25, [248].
\(^ {177}\) Convention art 24(1)(a). Internationally, the penalty level attached to international cooperation may vary from as low as six months to up to four years under the UNTOC. The more typical figure is 12 months: see Comprehensive Study on Cybercrime, above n 10, 62.
\(^ {178}\) Convention Explanatory Report, above n 25, [245].
\(^ {179}\) Convention art 24(1)(b).
\(^ {180}\) Comprehensive Study on Cybercrime, above n 10, 62.
\(^ {181}\) Convention art 24(5).
\(^ {182}\) European Convention on Extradition art 3.
\(^ {183}\) Extradition Act 1988 (Cth) s 22(3)(b).
\(^ {185}\) McKinnon v United States of America [2008] 4 All ER 1012; R (McKinnon) v Secretary of State for Home Affairs [2009] EWHC 2449 (Admin). His extradition was eventually blocked by the Home Secretary: ‘Gary McKinnon Extradition to US Blocked by Theresa May’, BBC News UK (online), 16 October 2012 <http://www.bbc.co.uk/news/uk-19957138>. See also Griffiths v United States of America (2005) 143 FCR 182.
Many states, particularly from the civil law tradition, do not extradite their own nationals, and in such cases the Convention recognises the principle of ‘aut dedere aut judicar’ — the obligation to extradite or prosecute. Where extradition is refused solely on the basis of nationality, or because the requested party claims jurisdiction over the case, then on request, the requested party must prosecute the matter under its domestic laws and report the outcome to the requesting party. If no request is made then there is no obligation on the party to undertake a domestic prosecution.

4 Territorial Sovereignty

While much of the criticism of the Convention has concerned the protection (or lack thereof) of individual rights, it has also been criticised for its lack of protection in relation to the rights of states. The nature of modern communications is such that data is increasingly ‘volatile, unstable and scattered over multiple jurisdictions’. The ability to access data in other jurisdictions expeditiously is therefore an important aspect of modern criminal investigations. While data in another jurisdiction may be accessed via more traditional means, including mutual assistance, the technology itself provides law enforcement agencies with the ability to conduct transborder searches; that is, ‘to unilaterally access computer data stored in another Party without seeking mutual assistance’. While such searches can be carried out covertly and deliberately, they may also be inadvertent or reckless; an inevitable consequence of networked computing. Because computer data may be stored anywhere in the world, simply accessing a webpage or an email account may involve the accessing of data stored in another country.

However the fact that law enforcement agencies (LEAs) have the capacity to conduct such searches does not make it lawful. It would ordinarily be regarded as a breach of territorial sovereignty for LEAs from one country to conduct investigations within a foreign country without the permission of that country. This principle of international law posits that no state may enforce its jurisdiction within the territory of another sovereign state. Accordingly, a state cannot enforce its laws, conduct investigations or arrest a person in the territory of another state, without clear legal authority to do so. Such conduct also threatens to undermine the protections accorded to the citizens of the target country. The

186 Manual on Mutual Legal Assistance and Extradition, above n 22, 49 [108]. See also Convention Explanatory Report, above n 25, [251].
187 Convention Explanatory Report, above n 25, [251].
188 Convention art 24(6).
189 Transborder Access and Jurisdiction Discussion Paper, above n 15, 9 [32].
190 Convention Explanatory Report, above n 25, [293].
legitimacy or otherwise of such conduct is therefore an issue of considerable importance.

The issue of transborder access to electronic evidence has been recognised since the 1980s, though at the time the issue did not seem ‘too pressing’. However, changes in technology meant that the issue rapidly became more urgent and was debated, inter alia, by the European Committee on Crime Problems, the G8 and the Council of Europe. Although the drafters of the Convention discussed the issue ‘at length’, agreement could not be reached other than in respect of two specific instances discussed below. This was apparently due to a lack of actual experience of such searches at the time, and the difficulty in formulating general principles when so much turns on the individual circumstances of the case.

The two instances of transborder search addressed by the Convention are found in art 32. The first states that a party may, without the authorisation of another party, ‘access publicly available (open source) stored computer data, regardless of where the data is located geographically’. This simply recognises that LEAs may access data in the same way as any member of the public, regardless of where that evidence is located.

The second and more controversial aspect is contained in art 32(b). It allows a party to ‘access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system’. Some countries, most notably Russia, have objected to this provision on the basis that it ‘might damage the sovereignty and security of member countries and their citizens’ rights’. The Russian attitude to this provision was undoubtedly not helped by the fact that Federal Bureau of Investigation agents were known to have conducted a covert transborder search of Russian computers in the course of their investigation against two Russian nationals — Alexey Ivanov and Vasily Gorshkov. Though often referred to in the context of the Convention, it is important to emphasise that art 32 says nothing of the situation that arose in that case, nor any covert transborder search. Accordingly, transborder searches not covered by the Convention are ‘neither authorised, nor precluded’ and the specific issue raised

193 *Transborder Access and Jurisdiction Discussion Paper*, above n 15, 6 [14].
194 Ibid 6–7 [15]–[17].
195 Convention Explanatory Report, above n 25, [293].
196 Ibid.
197 Convention art 32(a).
200 Convention Explanatory Report, above n 25, [293]. Convention art 39(3) provides that ‘[n]othing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party’.

---

*A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*
by the Ivanov/Gorshkov case remains unresolved and controversial. Therefore, objections to art 32(b) on the basis that it authorises such covert searches are misplaced.

This is not to say that art 32(b) is uncontroversial. By applying to both the accessing and receiving of data through a computer system with consent, it allows law enforcement in one country to conduct an extraterritorial investigation in another country without notifying authorities in that country. For example, the owner of an email account whose data is stored in another country may voluntarily disclose or allow access to that data to local law enforcement. The potential breadth of this provision becomes apparent when one considers that much of our modern communications networks and associated data storage is privately owned. ISPs and content providers such as Google and Facebook are repositories of enormous amounts of data, which may be of interest to LEAs. As long as the consent of the ‘owners’ of this data is obtained, it may lawfully be accessed by, or disclosed to, foreign LEAs.

The first limitation on the breadth of this provision is that consent must be voluntarily given. Clearly consent given as a result of duress, coercion or deception is not voluntary. Similarly, consent given by minors or persons with a cognitive impairment may also not be sufficient, subject to domestic law. A plain reading of the Convention would suggest that it authorises communications between LEAs in one country and individuals in another in order to obtain the necessary permission. However, for LEAs in one country to encourage a citizen of another country to assist with their investigations may itself be a breach of sovereignty and in some jurisdictions is a criminal offence. It has therefore been argued that art 32(b) can only be used to obtain the consent of a person who is under the jurisdiction of the investigating state. This accords with the Explanatory Report to the Convention (‘Convention Explanatory Report’), which gives the example of data stored outside the jurisdiction, where a person within the jurisdiction has lawful authority to retrieve that data. Where the person is present in the territory of another state, ‘mutual assistance procedures should be applied’.

The second limitation is that the person must have ‘lawful authority’ to consent to that data being accessed or received. As to the question of who has the ‘lawful authority’ to disclose, the Convention Explanatory Report rather obviously and unhelpfully states that this will depend on ‘the circumstances, the nature of the person and the applicable law concerned’. For example, lawful authority to

---

202 Convention Explanatory Report, above n 25, [294].
203 Transborder Access and Jurisdiction Discussion Paper, above n 15, 21 [104]–[105].
204 See, eg, Strafgesetzbuch [Swiss Criminal Code] (Switzerland) 21 December 1937, SR 311.0, art 271(1).
205 Kaspersen, above n 78, 28 [81].
206 Convention Explanatory Report, above n 25, [294].
207 Kaspersen, above n 78, 28 [81].
208 Convention Explanatory Report, above n 25, [294].
A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation

consent may reside in both the email user and the email provider, though different considerations will apply. To what extent does the service provider have authority to disclose that data? It has been suggested that in most parties, cooperation in a criminal investigation would require explicit consent and therefore ‘general agreement by a person to terms and conditions of an online service used would not constitute explicit consent even if these terms and conditions indicate that data may be shared with criminal justice authorities in cases of abuse’.

However, the terms of art 32 are not so limited.

Not only must the person have the lawful authority to disclose, that disclosure must itself be lawful. This serves to emphasise that it is for individual parties to determine the extent to which their citizens may lawfully disclose data. Concerns as to the potential broad sweep of this provision could be addressed, for example, by strict data protection laws. Note that the authority in art 32(b) is not simply to disclose the data, but to disclose to the party through a computer system. Therefore, restrictions on disclosure could be targeted to prohibit disclosure to foreign agencies.

While art 32 has the advantage of freeing up a large amount of data collection, and avoids the use of mutual legal assistance treaties, it is understandably a controversial provision. Given that it may be cited as a reason for not ratifying the Convention, it is imperative that it be addressed as was envisaged at the time of its drafting.

One option would be to remove art 32 from the Convention. Less drastic would be to allow parties to make a reservation to that provision. Yet another alternative would be to provide for a notification requirement. That is, where a country seeks to access or receive data under art 32(b), they must notify the party in which the person or organisation is resident. Although a limited notification requirement was proposed by the G8, it was not adopted in the Convention.

Such notifications should not slow down the process unless the requested party has an objection, in which case that objection should be resolved. Such requests are not covert, the requested person being under no obligation to keep the request confidential. Notification would also provide a level of supervision, which would help to address concerns as to voluntariness. It may be that such an approach addresses the concerns of countries otherwise reluctant to ratify on the basis of this provision.

209 Transborder Access and Jurisdiction Discussion Paper, above n 15, 21–2 [106].
210 See, eg, above n 198.
211 Transborder Access and Jurisdiction Discussion Paper, above n 15, 19 [90].
212 Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime (Communiqué, Moscow, 19–20 October 1999) annex 1 cl 6 <http://www.g8.utoronto.ca/adhoc/crime99.html> (‘Communiqué’). Of course, the Convention does not preclude parties providing notification if it is considered appropriate. See Transborder Access and Jurisdiction Discussion Paper, above n 15, 21 [103].
It could also be argued that this is an area where it may be appropriate to insert a protection of sovereignty clause as is found in some international agreements.\textsuperscript{213} For example, the \textit{UNTOC} requires parties to carry out their obligations under that Convention ‘in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States’.\textsuperscript{214} Further, parties are not entitled to undertake in another state ‘the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law’.\textsuperscript{215} A similar principle was in fact agreed upon by the G8 Justice and Interior Ministers meeting in Moscow in 1999,\textsuperscript{216} but was ultimately not included in the \textit{Convention}.

A further issue is that art 32(b) refers to ‘stored computer data located in another Party’. It is therefore presumed that that the location of the data is known.\textsuperscript{217} However, modern developments mean that this may no longer be the case, with data dynamically shifted — potentially between jurisdictions — such that it is impossible with certainty to state where particular data is at any one time.\textsuperscript{218} As it may be impossible for law enforcement agencies to determine whether data being accessed is stored locally or outside the jurisdiction,\textsuperscript{219} it may be necessary to develop mechanisms to address these new challenges.\textsuperscript{220}

More broadly, there is an ongoing need to address those transborder searches that fall outside the scope of art 32. A recent Council of Europe survey of member states indicates that transborder searches are occurring, though practices vary considerably.\textsuperscript{221} According to the United States Department of Justice, obtaining data from computers located overseas must ‘usually’ be in compliance with international treaties and mutual assistance requests.\textsuperscript{222} However, in some circumstances, investigators may argue that the search of data was justified by ‘exigent circumstances’, in particular the danger that evidence might be lost or destroyed.\textsuperscript{223} The extent to which such rationales can be used to justify access to data held in another jurisdiction is unclear.\textsuperscript{224}

\begin{flushleft}
215 \textit{UNTOC} art 4(2). See also \textit{UNCAC} art 4(2).
216 \textit{Transborder Access and Jurisdiction Discussion Paper}, above n 15, 6–7 [17]; Communiqué, above n 212, annex 1 cl 6.
217 Such a limitation does not apply to publicly accessible data, the location being irrelevant.
219 \textit{Transborder Access and Jurisdiction Discussion Paper}, above n 15, 18 [86].
221 \textit{Transborder Access and Jurisdiction Discussion Paper}, above n 15, 29 [137].
223 \textit{Transborder Access and Jurisdiction Discussion Paper}, above n 15, 9 [33]. See also ibid 27–31.
224 \textit{Transborder Access and Jurisdiction Discussion Paper}, above n 15, 10 [34].
\end{flushleft}
Apparent authority for such searches may come about due to broadly drafted search powers. For example, under *Crimes Act 1914* (Cth) s 3L, the executing officer of the warrant ‘may operate electronic equipment at the warrant premises to access data (including data not held at the premises)’. Although it may therefore be argued that the warrant authorises the officer to access data outside the jurisdiction, this provision is consistent with art 19(2) of the *Convention*, which applies where authorities search or access a specific computer system and believe on reasonable grounds that relevant data is stored in another system. In those circumstances, parties are required to empower authorities to extend the search to the other system. However, this only applies where the data is lawfully accessible from the initial system, and the other system is ‘in its territory’. It does not authorise an extraterritorial search. In any event, even if rendering the conduct lawful in Australia, it has no bearing on the legality of the conduct outside the jurisdiction.

**C (Un)representative**

The Council of Europe consists of 47 member states including all 27 members of the European Union. In addition, five countries have observer status: Canada, the Holy See, Japan, Mexico and the United States of America. Although representing a quarter of the world’s countries, they overwhelmingly represent the developed world, largely excluding the G24 and G77 groups of developing countries.

The *Convention* was always intended to apply globally, and in addition to member states and those who ‘participated in its elaboration’, it is open to non-member states invited by a unanimous decision of the parties. At the time of writing, only two member states had not signed — Russia and San Marino.

---

225 *Crimes Act 1914* (Cth) s 3L(1) (emphasis added).
226 This was also the position stated in the Revised Explanatory Memorandum, Cybercrime Bill 2001 (Cth) 15–16.
227 Although all 27 members of the European Union are members, the Council of Europe should not be confused with the European Council which is an institution of the European Union: see *Treaty of Lisbon*.
233 Clough, above n 37, 387.
235 *Convention* art 36(1).
236 Ibid art 37(1).
Two non-member countries — Canada and South Africa — have signed but not ratified, while thirteen others — Argentina, Chile, Colombia, Costa Rica, Israel, Mexico, Morocco, Paraguay, Peru, the Philippines, Senegal, Sri Lanka and Tonga — have been invited to sign.239

More significant than the number of signatories is the number of ratifications. While international obligations do not have the force of law in those countries adopting a dualist system until they are incorporated within domestic legislation, in monist systems, a treaty, once ratified, has the same authority as domestic law.240 In any event, once a treaty has been ratified, a party is bound by it notwithstanding that it is not incorporated into its domestic law.241 There are now only six member states which have signed but not ratified,242 and a number of non-member states have now ratified: the United States (2006), Australia and Japan (2012), Dominican Republic and Mauritius (2013) and Panama (2014).243

This brings to 45 the number of parties to the Convention who have ratified. While obviously falling short of truly international agreement, no equivalent initiative exists, let alone comes close to this level of international acceptance.244 Rather than looking at overall numbers of ratifications, it is important to consider why particular countries may not have ratified.

An obvious impediment is that, in contrast to United Nations conventions,245 accession for non-member states is by invitation and requires a majority decision of the Committee of Ministers of the Council of Europe, albeit with the unanimous consent of all parties.246 Although it may be difficult for some countries to ratify a convention that they did not participate in drafting, such mechanisms are not unique.247 Further, the process of invitation does at least help to ensure genuine implementation,248 and those who become parties become members of the Cybercrime Convention Committee and are involved in its future development.249

---

239 Council of Europe, Convention on Cybercrime CETS No: 185, above n 237.
240 Manual on Mutual Legal Assistance and Extradition, above n 22, 10 [23]–[24].
242 Andorra, Greece, Ireland, Liechtenstein, Monaco and Sweden: Council of Europe, Convention on Cybercrime CETS No: 185, above n 237.
243 Ibid.
244 See Part V below.
245 Gerecke, ‘10 Years Convention on Cybercrime’, above n 37, 145.
246 Convention art 37.
248 Although the Convention provides no mechanism for ensuring compliance with its terms, and some have not been fully implemented even by those who have ratified: Gerecke, ‘10 Years Convention on Cybercrime’, above n 37, 145.
249 Convention, art 46; Council of Europe, Cybercrime Convention Committee (T-CY) <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp>.
Further, many parties have exercised their right under the Convention to declare reservations, thereby allowing its implementation to be adapted to local conditions. While this may dilute uniformity, reservations allow for differences to be accommodated in a transparent and coherent fashion, and are an accepted way of addressing the difficulties in achieving international consensus.

More broadly, for many countries non-ratification is a capacity issue. The Convention requires countries to have in place domestic legislation across the spectrum of substantive and procedural laws and to put in place mechanisms for international cooperation. These measures can present significant capacity challenges for developed countries. For developing countries, those challenges may be insurmountable without assistance.

Even for countries that have the capacity to ratify, there may be serious political objections which are seen to outweigh the benefits of the Convention. For example, Russia’s non-acceptance is based in part on objection to a particular provision rather than a wholesale rejection. In Canada, the process has been hampered by an inability to pass domestic legislation. For some countries the level of human rights protection may be too low, for others too high. None of these necessarily represent a failure of the Convention, but rather illustrate the challenges of implementing such a comprehensive international instrument. These same challenges would be faced in implementing any international convention.

### III A UNITED NATIONS CONVENTION ON CYBERCRIME?

#### A ‘The Perfect is the Enemy of the Good’

Despite near universal support for international action against cybercrime, there is currently no binding international cybercrime agreement. If the Convention is not to fulfil this role, the question arises as to how such international consensus

---


252 As to some of the legislative challenges even within Europe, see Anne Flanagan, ‘The Law and Computer Crime: Reading the Script of Reform’ (2005) 13 *International Journal of Law and Information Technology* 98.

253 Alexander Seger, ‘The Budapest Convention on Cybercrime 10 Years on: Lessons Learnt or the Web is a Web’ (Council of Europe, 16 February 2012) 5.


256 The original quote in French is ‘Le mieux est l’ennemi du bien’, from Voltaire, *Dictionnaire Philosophique, Portatif* (Cramer, 1764).

257 *Comprehensive Study on Cybercrime*, above n 10, 64.
is to be achieved. The United Nations is the obvious choice, with its resolutions on *Combating the Criminal Misuse of Information Technologies* raising many of the issues addressed by the *Convention*. However, none of these measures were binding, with member states invited to take them into account in developing their own efforts to combat the criminal misuse of information technologies.

Out of the first phase of the World Summit on the Information Society, held in Geneva in 2003 came the *Geneva Declaration of Principles* and the *Geneva Plan of Action*. The latter included action line C5, ‘Building Confidence and Security in the use of ICTs’, art 12(b) of which contained a number of measures that government should take, in cooperation with the private sector, to ‘prevent, detect and respond to cyber-crime and misuse of ICTs’. The second phase held in 2005 produced the *Tunis Agenda for the Information Society*. In the context of legislative reform, this called upon governments ‘to develop necessary legislation for the investigation and prosecution of cybercrime’ taking into account existing frameworks and regional initiatives ‘including, but not limited to, the Council of Europe’s *Convention on Cybercrime*’.

In 2007 the International Telecommunication Union (ITU), which is responsible for facilitating action line C5, launched its Global Cybersecurity Agenda (GCA). The GCA is divided into five pillars/work areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation. In respect of legal measures it highlights the importance of international harmonisation and, in what would seem a thinly veiled reference to the *Convention*, notes that ‘[s]ome efforts to address this challenge have been undertaken, and although very valuable, they are still insufficient. The Internet is an international communication tool and, consequently, any solution to secure it must be sought at the global level’.

Yet the GCA does not pursue a binding global initiative. The first of the seven strategic goals ‘calls for the elaboration of strategies for the development of cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures’. Harmonisation of laws and facilitation of international cooperation is seen as essential to achieving global

---

258 *Combating Criminal Misuse No 1*, UN Doc A/RES/55/63; *Combating Criminal Misuse No 2*, UN Doc A/RES/56/121.
259 *Combating Criminal Misuse No 1*, UN Doc A/RES/55/63, para 1.
260 Ibid para 2; *Combating Criminal Misuse No 2*, UN Doc A/RES/56/121, para 2.
265 *Tunis Agenda for the Information Society*, above n 113, [40].
267 Ibid 12.
268 Ibid 14.
269 Ibid.
cybersecurity.\textsuperscript{270} However, the mechanism whereby such harmonisation can be achieved remains contested. The \textit{Convention} is the only non-United Nations initiative referred to by the General Assembly as a regional initiative to which countries should have regard in ascertaining whether they have developed the necessary legislation for the investigation and prosecution of cybercrime.\textsuperscript{271}

The Twelfth United Nations Congress on Crime Prevention and Criminal Justice produced a clear division of opinion as to whether to proceed with negotiation of a global convention on cybercrime.\textsuperscript{272} On the one hand, countries such as the Russian Federation\textsuperscript{273} and China supported the negotiation of a global convention.\textsuperscript{274} The broader notion of an international agreement also finds support in African,\textsuperscript{275} Asian and Pacific,\textsuperscript{276} Latin American and Caribbean\textsuperscript{277} nations. On the other hand, the United States, United Kingdom\textsuperscript{278} and European Union\textsuperscript{279} argued that the \textit{Convention} is sufficient and that the focus should be on capacity building.

The Commission on Crime Prevention and Criminal Justice was then invited to convene ‘an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime’.\textsuperscript{280} In addition, it was recommended ‘that the United Nations Office on Drugs and Crime, upon request,

\textsuperscript{270} Ibid.

\textsuperscript{271} Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures, GA Res 64/211, UN GAOR, 64\textsuperscript{th} sess, 66\textsuperscript{th} plen mtg, Agenda Item 55(e), UN Doc A/RES/64/211 (17 March 2010, adopted 21 December 2009).


\textsuperscript{273} See generally Ernest, above n 213.


\textsuperscript{278} Masters, above n 274. The Quintet of Attorneys-General from Australia, Canada, New Zealand, the United Kingdom and the United States have resolved to ‘promote the \textit{Convention} as the key international instrument for dealing with cyber crime and use the \textit{Convention} as a basis for delivering capacity building and awareness raising activities’: US Reference Service, Communiqué — Quintet of Attorneys General: Action Plan to Fight Cyber Crime (18 August 2011) <http://usrsaustralia.state.gov/us-oz/2011/07/15/aag2.html>.

\textsuperscript{279} Proposal on Attacks against Information Systems, above n 45, 6–7.

provide, in cooperation with Member States, relevant international organizations and the private sector, technical assistance and training’ in order to deal with cybercrime.281

Most recently, the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study of the Problem of Cybercrime (‘Expert Group’) met in January 2011,282 and again in February 2013, at which time it considered the United Nations Office on Drugs and Crime’s Comprehensive Study on Cybercrime.283 In December 2012, the United Nations General Assembly noted with appreciation the work of the Expert Group, and encouraged it ‘to enhance its efforts to complete its work and to present the outcome of the study to the Commission on Crime Prevention and Criminal Justice in due course’.284 At the subsequent meeting of the Commission on Crime Prevention and Criminal Justice in April 2013, the issue of international agreement was once again deferred, with a draft resolution inviting member states ‘to continue to consider … ways and means to strengthen international cooperation in combating cybercrime’, and requesting an open-ended intergovernmental working group to be convened to further examine the problem of cybercrime and responses to it by member states.285 A further draft resolution requested the United Nations Office on Drugs and Crime (UNODC) ‘to strengthen partnerships for technical assistance and capacity-building with Member States, relevant organizations, the private sector and civil society’, and ‘to serve as a central repository of cybercrime laws and good practices’.286 Although over 10 years has passed since the idea was seriously mooted,287 we are no closer to a United Nations convention nor to international acceptance of the Convention.

There are a number of advantages to pursuing a convention through the United Nations. The first and most significant is that it would have the broadest geographic scope, being open to all member states.288 Second, it would provide an opportunity to address issues not included in the Convention, or to improve on provisions requiring amendment.289 Third, it would potentially allow amendment

281 Salvador Declaration para 41.


287 Downing, above n 37, 761.

288 Comprehensive Study on Cybercrime, above n 10, 66–7.

289 Clough, above n 37, 389.
or removal of the provisions that have provided an obstacle to wider acceptance of the *Convention*.

There are, however, a number of significant disadvantages. Principal among them is the time taken to reach international agreement, if agreement can in fact be reached. It has been estimated that having signed the *Convention* it takes a country, on average, more than five years to ratify.\(^{290}\) Should a comprehensive binding international cybercrime agreement be implemented, there is no reason to believe that ratification would occur more quickly. In an area where we are constantly told of how rapidly technology outpaces attempts at regulation, there seems to be a blithe acceptance that we can wait a few more years before international agreement is reached.

Even assuming international agreement can be reached, it is not clear that it would add a great deal to the *Convention*. In fact, in order to ensure international agreement it is likely to provide less. The influence of the *Convention* ‘has now been so pervasive on cybercrime laws throughout the world that any international agreement would largely have to mirror its terms’.\(^{291}\) Were it to depart significantly, it would be unlikely to achieve agreement from those countries that have implemented legislation based on the *Convention*. Equally, to ensure agreement from those countries that have objected to terms of the *Convention*, it would need to provide less. Human rights and privacy protections, for example, may have to be diluted or removed, while certain substantive offences may not be included.\(^{292}\)

As an illustration of the difficulties of achieving international agreement in this area, as recently as 2012 agreement could not be reached on the International Telecommunication Regulations.\(^{293}\) Although signed by 89 member states, a number of countries including Australia, Canada, the United Kingdom and the United States refused to sign,\(^{294}\) in part due to an addition to the preamble proposed by African countries which states that ‘[t]hese regulations recognise the right of access of member states to international telecommunication services’.\(^{295}\) This was seen by some countries as expanding the regulations beyond their current remit to cover Internet governance and content.\(^{296}\)

---

290 Gercke, ‘10 Years Convention on Cybercrime’, above n 37, 144.
291 Clough, above n 37, 389.
292 The ITU Cybercrime Toolkit, for example, does not contain provisions related to child pornography: International Telecommunication Union, ‘ITU Toolkit for Cybercrime Legislation’ (Draft Rev February 2010) 32–3 (‘ITU Toolkit’).
295 ‘US and UK Refuse to Sign UN’s Communications Treaty’, above n 294.
296 Ibid.
IV (DIS)HARMONY

Overall, the global picture is one of a certain degree of fragmentation in membership of international and regional instruments related to cybercrime. Regional patterns are particularly clear. Countries in some parts of the world benefit from membership of binding cybercrime instruments — including more than one instrument for some countries — while other regions do not participate in any binding framework. 297

An international convention is, of course, only one approach to harmonisation, and recent years have seen a flurry of activity in relation to cybercrime at the international, regional and national level. The UNODC has identified five ‘clusters’ of international and regional instruments addressing the challenges of cybercrime. 298

The first are those which have been developed in the context of the Convention, the most significant being the Commonwealth Model Law on Computer and Computer Related Crime. 299 Second, those developed by the Commonwealth of Independent States (CIS) 300 and the Shanghai Cooperation Organisation (SCO). 301 The third is the League of Arab States’ Arab Convention on Combating Information Technology Offences 302 and associated Model Law. Fourth is the Draft African Union Convention on the Establishment of a Legal Framework Conducive to Cyber Security in Africa. 303 If ratified, this last instrument will make a particularly significant contribution to the development of cybercrime.

297 Comprehensive Study on Cybercrime, above n 10, 68.
298 Ibid 64.
laws globally, being a binding instrument which encompasses the 54 member states of the African Union.\(^{304}\)

The fifth category is United Nations instruments. Although there is no United Nations convention on cybercrime, the UNTOC can and has been utilised in the context of cybercrime.\(^{305}\) The UNTOC applies to the ‘prevention, investigation and prosecution’ of a number of specific offences required to be criminalised under arts 5, 6, 8 and 23,\(^{306}\) as well as ‘serious crime’\(^{307}\) where the offence is ‘transnational in nature and involves an organized criminal group'.\(^{308}\) The UNTOC has been ratified by 181 countries\(^{309}\) and requires parties to ‘afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings’.\(^{310}\) It may also be used as the basis for extradition in those cases to which it applies.\(^{311}\)

Although the United Nations’ Model Treaty on Mutual Assistance in Criminal Matters\(^{312}\) and Model Treaty on Extradition\(^{313}\) do not deal specifically with cybercrime investigations or prosecutions, they can be applied or adapted to computer searches.\(^{314}\) For example, the revised Model Law on Mutual Assistance in Criminal Matters\(^{315}\) contains model provisions for expedited preservation and disclosure of stored computer data, production of stored computer data and search and seizure of computer data.\(^{316}\) They do not, however, contain provisions relating


\(^{305}\) See Catalogue of Cases, UN Doc CTOMIC/COP/2010/CRP.5, 6 [27].

\(^{306}\) UNTOC art .4(1). These are offences relating to participation in an organised criminal group, laundering of proceeds of crime, corruption and the obstruction of justice.

\(^{307}\) Defined as ‘conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty’: ibid art 2(b).

\(^{308}\) Ibid art 3(1)(b).


\(^{310}\) UNTOC art 18(1).

\(^{311}\) Ibid arts 16 (extradition), 18 (mutual legal assistance). See also Manual on Mutual Legal Assistance and Extradition, above n 22, 2 [3].


\(^{314}\) UNODC Revised Manuals, above n 79, 70 [12(d)], 77–8 [42], 111–12 [169].


\(^{316}\) Ibid ch 2 pt 4.
to electronic surveillance and interception, these being matters which parties may consider including in any treaty between them.\footnote{317}{UNODC Revised Manuals, above n 79, 79 [47].}

These are, of course, not discrete clusters, and there is considerable overlap. The \textit{Convention}, in particular, has played a significant role in influencing the drafting of other instruments. In the Commonwealth, for example, beyond those countries which are parties, the \textit{Convention} and the \textit{Commonwealth Model Law on Computer and Computer Related Crime} have influenced the cybercrime legislation of a significant number of countries.\footnote{318}{See discussion on Commonwealth States’ use of the Convention: Council of Europe, ‘Cybercrime Legislation of Commonwealth States’, above n 299. At the meeting of Commonwealth Law Ministers in Sydney in 2011, ministers mandated the Commonwealth Secretariat to form a multidisciplinary working group of experts to review the practical implications of cybercrime in the Commonwealth [and] identify the most effective means of international co-operation and enforcement, taking into account, amongst others, the Council of Europe \textit{Convention on Cybercrime}, without duplicating the work of other international bodies … Commonwealth Working Group of Experts on Cybercrime, ‘Report to Commonwealth Law Ministers 2014 (Report, Commonwealth Secretariat, 2014).\textit{}} Its influence further extends to countries such as Argentina, Pakistan, the Philippines, Egypt, New Zealand\footnote{320}{And Nigeria.\textit{}} and Nigeria.\footnote{321}{Adoption of the Convention has been recommended by the Organization of American States\footnote{322}{2014 (Report, Commonwealth Secretariat, 2014).\textit{}} and the Financial Action Task Force,\footnote{323}{and its influence on the United Nations’ ITU Toolkit\footnote{324}{2012.\textit{}} further expands its reach. Even within Russia it is acknowledged as the ‘most important international legal instrument aimed at combating crime against computer security’.\textit{}} Overall it is claimed to have influenced approximately 100 countries in the drafting of their cybercrime laws,\footnote{326}{though such claims are very difficult to verify, and may conceal considerable divergence in levels of implementation.\textit{}}

\begin{itemize}
\item \textit{ITU Toolkit\textit{, above n 292.}\textit{}}
\item \textit{Ernest, above n 213, slide 18.}\textit{}}
\end{itemize}
Beyond the *Convention*, the ITU has been active in promoting model legislation in a number of areas including Africa, the Caribbean, and the Pacific. Africa, in particular, has seen a raft of initiatives, including the East African Community’s *Draft EAC Legal Framework for Cyberlaws*,328 the Economic Community of West African States’ *Directive on Fighting Cyber Crime Within ECOWAS*,331 the Common Market for Eastern and Southern Africa’s (COMESA) *Cybersecurity Draft Model Bill (2011)*332 and the South African Development Community’s *Computer Crime and Cybercrime Model Law*.333

Although it is positive to see so many global initiatives addressing the challenges of cybercrime, there is the very real danger of fragmentation. While a comparative analysis is beyond the scope of this article,334 it is sufficient to note that there are significant differences. For example, while the *Convention*, the *Commonwealth Model Law on Computer and Computer Related Crime*, the CIS Agreement and the *Arab Convention* all focus on a criminal justice response to cybercrime,335 others address cybercrime as part of a broader attempt to deal with international information security.336 The *Draft African Union Convention* for example, includes provisions relating to electronic transactions, cybersecurity and e-governance as well as cybercrime.337 Similarly, the SCO’s *Agreement on Cooperation in the Field of Information Security* provides for international cooperation in relation to information warfare, terrorism and other threats to international information infrastructure.338 Even within a criminal justice response, only the *Convention* and the *Arab Convention* cover substantive law, procedural law, jurisdiction and mutual assistance.339 Some provide for substantive offences on which it would be difficult to obtain broad international agreement, such as pornography and public order offences.340 Electronic evidence, which is vital to successful cybercrime prosecutions, is covered by relatively few instruments.341

---

332 *Comprehensive Study on Cybercrime*, above n 10, 64.
334 For a comparative analysis see *Comprehensive Study on Cybercrime*, above n 10, annex 3 267–75.
335 Ibid 68.
336 Ibid.
337 Ibid 69.
338 Ibid 68–9.
339 Ibid 70.
340 Ibid.
341 See ibid 69.
V WHERE TO FROM HERE?

Ultimately, however, the use of both binding and non-binding international and regional instruments has significant potential for positive progress towards greater sufficiency and harmonization of national laws — and, in the long run, enhanced international cooperation against a global challenge.342

On the one hand, the current global situation is one in which cybercrime is clearly on the international agenda, with a broad range of international, regional and national models for countries to draw upon. On the other hand, there is the danger that divergence ‘may lead to the emergence of country cooperation “clusters” that are not always well suited to the global nature of cybercrime’.343 While the United Nations process continues, it is conceivable that no international agreement will be reached on this issue in the near future. An international agreement will face the same challenges as the Convention — plus the additional issues that it does not address — all to be agreed between the member states of the United Nations. The ‘window of opportunity’ during which such an agreement could be reached may have passed,344 and it would now be ‘very difficult to bring all interests under an international agreement of the scope and depth of the Budapest Convention’.345

In the absence of international agreement, the Convention remains ‘the most complete international standard to date’.346 As of 2013, 82 countries had signed and/or ratified a binding cybercrime instrument.347 While no one instrument could be said to have global reach, the Convention has by far the largest influence,348 with 53 signatures/ratifications.349 Although falling short of a ‘global standard’,350 amongst countries responding to the UNODC’s Comprehensive Study on Cybercrime it has by far the greatest influence on existing or planned cybercrime legislation.351

This is not to suggest that all countries should accede to the Convention. The reality is that many will not or cannot. The Convention does, however, provide an important touchstone against which a country’s response to cybercrime may be measured, providing a ‘guideline or reference’ even for those countries which do not want to become parties.352

342 Ibid 76.
343 Ibid xi.
344 Seger, above n 253, 3.
345 Ibid.
346 Proposal on Attacks against Information Systems, above n 45, 3.
347 Comprehensive Study on Cybercrime, above n 10, 67.
348 Ibid.
349 Council of Europe, Convention on Cybercrime CETS No: 185, above n 237. Compare with the Arab Convention (18 countries/territories), CIS (10 countries/territories) and SCO (six countries/territories).
350 Gercke, ‘10 Years Convention on Cybercrime’, above n 37, 144.
351 Comprehensive Study on Cybercrime, above n 10, 75.
352 Seger, above n 253, 5.
Perhaps the most promising development over recent years has been the increased emphasis on capacity building, and the willingness of international, regional and national agencies to assist countries in developing an appropriate response to cybercrime. At the international level, there is increased cooperation between the UNODC and other relevant organisations including INTERPOL, the ITU, the European Commission and the Council of Europe, as well as the private sector.\(^\text{353}\)

In 2012, the UNODC finalised its ‘Global Programme on Cybercrime’ which is intended to take an ‘holistic approach’ including ‘enhanced national, regional and international cooperation in addressing cybercrime’.\(^\text{354}\) In this it is supported by the ITU\(^\text{355}\) whose Cybersecurity Gateway lists a range of initiatives drawing upon the expertise of national, regional and international agencies and bodies.\(^\text{356}\) In addition, the ITU has produced two resources, the ITU Toolkit\(^\text{357}\) and Understanding Cybercrime: Phenomena, Challenges and Legal Response.\(^\text{358}\) The UNODC also participates as an observer with the Council of Europe Convention Committee, the Commonwealth Cybercrime Initiative and others.\(^\text{359}\)

The ‘Octopus’ programme is part of the Council of Europe’s ‘Global Project on Cybercrime’.\(^\text{360}\) The ‘Octopus Conference’ on cybercrime was first run in 2007 to encourage ratification and accession to the Convention and aimed to promote the use of the Convention as a guide in developing national legislation.\(^\text{361}\) Today the conference still addresses the implementation of the Convention and ‘threats and trends’ in cybercrime, but also takes a unique focus each year.\(^\text{362}\) For instance, in 2012 the key focuses of the conference were jurisdiction and cloud computing and information sharing.\(^\text{363}\) The Council of Europe also facilitates the ‘Octopus

---


354 Ibid 2 [4].


357 See generally ITU Toolkit, above n 292.


359 Promotion of Activities Relating to Combating Cybercrime, UN Doc E/CN.15/2013/24, [13]–[14].


363 Council of Europe, Octopus 2012, above n 362.
Cybercrime Community’, which links cybercrime experts from around the globe with an aim of strengthening cooperation against cybercrime.364

To see harmonisation as a destination is unrealistic; it is a process. As the technology evolves and changes so too our responses will need to evolve and change. The ideal that all member states will have comprehensive cybercrime laws is a noble goal, but one that is many years off. With almost 60 per cent of reporting countries in the UNODC’s Comprehensive Study on Cybercrime indicating new or planned cybercrime legislation,365 it is vital that support be provided. Rather than focusing on differences as an impediment to harmonisation, the focus should be on how those differences may be resolved in working towards the common goal of effective international cooperation against a global challenge.

The binary debate about the Convention versus a United Nations Convention in some way presents a false dichotomy. Each country will determine what it considers necessary to effectively combat cybercrime, looking to national, regional and international standards in enacting laws that best suit its national circumstances. Nonetheless, the Convention provides a crucial benchmark against which such efforts can be measured, providing an internationally recognised framework for the harmonisation of cybercrime laws. For those countries that are unable to, or choose not to ratify, it provides an important model against which their own laws can be compared. Discussions about what the Convention does not cover are equally important for parties and non-parties alike. The UNODC and Council of Europe, as well as other regional and national initiatives, play an extremely valuable role in information sharing and capacity building. In this way, difference and diversity becomes a driver of change; the focus on what needs to be achieved rather than how difficult it will be. In a world now connected by technology, we may find that ‘[w]hat unites us is far greater than what divides us’.366

364 Council of Europe, Welcome to the Octopus Cybercrime Community: About the Octopus Cybercrime Community <http://octopus-web.ext.coe.int>.
365 Comprehensive Study on Cybercrime, above n 10, 63.