CyberCrime@IPA

EU/COE Joint Project on Regional Cooperation against Cybercrime

www.coe.int/cybercrime

Data Protection and
Cybercrime Division
Directorate General of
Human Rights and Rule of Law
Strasbourg, France

Version 8 November 2011
(Draft for discussion)

Article 15
Conditions and Safeguards
under the
Budapest Convention on Cybercrime

Discussion paper
with contributions by
Henrik Kaspersen (Netherlands)
Joseph Schwerha (USA)

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

CONTENT

For further information please contact:

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe
Strasbourg, France

Tel: +33-3-8841-2103
Fax: +33-3-9021-5650
Email: cristina.schulman@coe.int
www.coe.int/cybercrime

1 Background and context

1.1 Purpose and structure of the report

The Budapest Convention on Cybercrime not only requires Parties to this treaty to criminalise conduct such as illegal access, data and system interference, child pornography and other offences in their domestic legislation but also to provide their law enforcement authorities with effective tools to investigate cybercrime and collect electronic evidence.

According to Article 15, the procedural powers adopted by Parties to the Convention are to be "subject to conditions and safeguards provided for under its domestic law which shall provide for the adequate protection of human rights and liberties..." Article 15 establishes principles and requirements to ensure that governments meet their positive obligation to protect people and their rights against cybercrime while at the same time respecting their fundamental rights when investigating crime.

The Council of Europe addresses this question when supporting countries in the implementation of the Budapest Convention through its capacity building programme on cybercrime. This programme includes joint projects of the Council of Europe and the European Union. A major joint project is CyberCrime@IPA on cooperation against cybercrime in South-eastern Europe, covering Albania, Bosnia and Herzegovina, Croatia, Montenegro, Serbia, "The former Yugoslav Republic of Macedonia", Turkey and Kosovo.[1]

CyberCrime@IPA is designed to make sure that policy- and decision-makers are aware of human rights implications when taking measures against cybercrime. Policies, legislation and other measures are to be compliant "with the European Convention on Human Rights, Article 15 of the Budapest Convention and relevant case law of the European Court of Human Rights".[2]

During the inception phase of the project between November 2010 and February 2011, a "situation report" was prepared assessing the state of measures against cybercrime in the eight project areas, including an overview of law enforcement powers under procedural law and the corresponding conditions and safeguards. This issue was furthermore addressed during a regional workshop on cybercrime legislation in Sarajevo (Bosnia and Herzegovina) in March 2011.

Obviously, the question of the appropriate "balance" between law enforcement powers and the rights of individuals is of great public interest and subject to controversial debates not only in South-eastern Europe.[3]

The purpose of the present report therefore is to further advance the discussion on this complex issue by sharing experience in the project region and beyond. It may help "operationalise" the general principles of Article 15 in view of assessing and supporting their implementation in different countries.

Following introductory sections on the procedural powers and related conditions and safeguards of the Budapest Convention, Professor Henrik Kaspersen and Professor Joseph Schwerha present in their contributions how Article 15 is applied in the Netherlands and the USA respectively. Both

[1] All reference to Kosovo, whether to the territory, institutions or population, in this text shall be understood in full compliance with United Nations Security Council Resolution 1244 and without prejudice to the status of Kosovo.

[2] See expected result 1 and activity 1.2.

[3] It was discussed for example at the 2010 Octopus conference (http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Interface2010_en.asp) and at different meetings of the Internet Governance Forum (including in Nairobi in September 2011).

examples illustrate why the practical implementation of Article 15 cannot be regulated in detail in an international treaty but must be left to domestic law, practice and judicial systems.

1.2 Procedural powers provided by the Budapest Convention

Articles 14 to 21 of the Budapest Convention cover procedural law, that is, investigative powers of law enforcement.[4] Article 14 defines the scope of procedural provisions and article 15 stipulates "that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law". The safeguards and conditions, in particular of article 15, will be explained further below. They are to be applied with respect to the following powers:

Article 16 – Expedited preservation of stored computer data	This provision is to enable "competent authorities to order or similarly obtain the expeditious preservation of specified[5] computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification"
Article 17 – Expedited preservation and partial disclosure of traffic data	This is to ensure that it is possible to preserve traffic data "regardless of whether one or more service providers were involved in the transmission of that communication". Therefore, "a sufficient amount of traffic data" is to be disclosed "to enable the Party to identify the service providers and the path through which the communication was transmitted"
Article 18 – Production order	This is necessary to empower competent authorities to order: "a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control."
Article 19 – Search and seizure of stored computer data	This is a rather detailed article "to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory." Other provisions of this article include that if the competent authorities in the course of a law search "have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system."
Article 20 – Real-time collection of traffic data	This article is to empower "competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the

[4] This table summarises the provisions. It is advisable to consult the full text of the Convention as well as the Explanatory Report (www.coe.int/cybercrime).

[5] Note: this is about "specified" data and is not be confused with a general data retention requirement.

	collection or recording of, traffic data, in real-time, associated with specified[6] communications in its territory transmitted by means of a computer system." In order not to compromise an investigation, it also foresees "measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it."
Article 21 – Interception of content data	This article is to empower "competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system." In order not to compromise an investigation, it also foresees "measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it."

With regard to articles 16 to 21, for each article it is stated that "the powers and procedures referred to in this article shall be subject to Articles 14 and 15".

Chapter III (articles 23 to 35) of the Convention covers international cooperation. Some of the procedural law provisions to be taken at the domestic level have their equivalent in this chapter:

- Article 29 – Expedited preservation of stored computer data
- Article 30 – Expedited disclosure of preserved traffic data
- Article 31 – Mutual assistance regarding accessing of stored computer data
- Article 32 – Trans-border access to stored computer data with consent or where publicly available
- Article 33 – Mutual assistance in the real-time collection of traffic data
- Article 34 – Mutual assistance regarding the interception of content data

The international cooperation provisions also refer back to domestic conditions and procedures. For example:

Article 33 – Mutual assistance in the real-time collection of traffic data	1 "The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case."
Article 34 – Mutual assistance regarding the interception of content data	"The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws. "

[6] Again: this is not about a blanket collection of traffic data but refers to "specified communications".

1.3 Conditions and safeguards

1.3.1 Procedural safeguards under the Budapest Convention

1.3.1.1 Preamble

The Preamble of the Budapest Convention states the need for a balance between law enforcement interests and respect for fundamental human rights as well as the right to the protection of personal data:

> "Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;"
>
> "Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;"

1.3.1.2 Substantive law

The substantive criminal law articles (ranging from article 2 "Illegal access" to article 10 "offences related to infringements of copyright and related rights" and ancillary liability such as article 11 "attempt and aiding or abetting") are formulated cautiously to avoid over-criminalisation. Some articles allow for additional reservations or declarations, although limitations such as proof of "dishonest intent", may render provisions less effective. With respect to:

- Article 2 ("illegal access") a Party may require that "the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent"
- Article 4 ("data interference") that "the conduct result in serious harm"
- Article 7 ("computer-related forgery"), "a Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches"
- Article 10 (IPR offences), that "acts are committed willfully" and "on a commercial scale".

Conditions and safeguards, however, apply primarily to the investigative powers, that is, to procedural law.

1.3.1.3 Scope of procedural provisions (article 14)

Article 14 defines the "scope of procedural provisions". The powers and procedures are to be applied to:

> "a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
> b other criminal offences committed by means of a computer system; and
> c the collection of evidence in electronic form of a criminal offence."

The scope of these provisions is, therefore, very broad and does not only cover the offences under the Convention (articles 2 to 11) but any offence by means of computers or involving electronic

evidence. However, there are two exceptions and these concern articles 20 ("real-time collection of traffic data") and article 21 ("interception of content data"). As the interception of content (article 21) is considered one of the most intrusive powers, and thus to meet the principle of proportionality, Parties should limit this measure to a range of serious offences:

> "1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law ... "

It is to be applied to "specified communications in its territory transmitted by means of a computer system".

In many countries, a distinction is made between traffic and content data, the latter being given a higher level of protection. However, where both types of data are treated the same way, a Party may reserve the right to limit article 20 to a range of serious offences as long this is not more limited than the offences to which article 21 is applied.[7]

1.3.1.4 Article 15[8]

The main provision of the Budapest Convention regarding safeguards and conditions is Article 15. The text reads as follows:

> Article 15 – Conditions and safeguards
>
> 1 Each Party shall 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 under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
>
> 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
>
> 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

[7] See para 142-144 of the Explanatory report of the Budapest Convention.

[8] Henrik Kaspersen and Joseph Schwerha, in their contributions, also contain explanations of Article 15 from different perspectives: Henrik Kaspersen from that of one of the main drafters of the Convention and its explanatory report, and Joseph Schwerha from a US perspective. All of this will enrich the understanding of Article 15.

The Explanatory Report helps interpret this article:[9]

> 145. The establishment, implementation and application of the powers and procedures provided for in this Section of the Convention shall be subject to the conditions and safeguards provided for under the domestic law of each Party. Although Parties are obligated to introduce certain procedural law provisions into their domestic law, the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. These domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise. The modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure. Parties shall ensure that these conditions and safeguards provide for the adequate protection of human rights and liberties. There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments. These instruments include the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and its additional Protocols No. 1, 4, 6, 7 and 12 (ETS N°s 005, 009, 046, 114, 117 and 177), in respect of European States that are Parties to them. It also includes other applicable human rights instruments in respect of States in other regions of the world (e.g. the 1969 American Convention on Human Rights and the 1981 African Charter on Human Rights and Peoples' Rights) which are Parties to these instruments, as well as the more universally ratified 1966 International Covenant on Civil and Political Rights. In addition, there are similar protections provided under the laws of most States.
>
> 146. Another safeguard in the convention is that the powers and procedures shall "incorporate the principle of proportionality." Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures. Also, the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle.
>
> 147. Without limiting the types of conditions and safeguards that could be applicable, the Convention requires specifically that such conditions and safeguards include, as appropriate in view of the nature of the power or procedure, judicial or other independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or the duration thereof. National legislatures will have 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. As stated in Paragraph 215, Parties should clearly apply conditions and safeguards such as these with respect to interception, given its intrusiveness. At the same time, for example, such safeguards need not apply equally to preservation. Other safeguards that should be addressed under domestic law include the right against self-

[9] The Explanatory Report is not a binding text but nevertheless a source of interpretation.

incrimination, and legal privileges and specificity of individuals or places which are the object of the application of the measure.

148. With respect to the matters discussed in paragraph 3, of primary importance is consideration of the "public interest", in particular the interests of "the sound administration of justice". To the extent consistent with the public interest, Parties should consider other factors, such as the impact of the power or procedure on "the rights, responsibilities and legitimate interests" of third parties, including service providers, incurred as a result of the enforcement measures, and whether appropriate means can be taken to mitigate such impact. In sum, initial consideration is given to the sound administration of justice and other public interests (e.g. public safety and public health and other interests, including the interests of victims and the respect for private life). To the extent consistent with the public interest, consideration would ordinarily also be given to such issues as minimising disruption of consumer services, protection from liability for disclosure or facilitating disclosure under this Chapter, or protection of proprietary interests.

1.3.2 Relevant international human rights standards

As pointed out in the Explanatory Report, since safeguards and conditions are governed by domestic law and since Parties to the Convention represent "many different legal systems and cultures", the conditions and safeguards cannot be defined in detail. However, Parties must adhere to certain principles. "These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments".

For member States of the Council of Europe the main instrument applicable is the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Protocols to which they are Party, as well as the case law of the European Court of Human Rights.[10]

While these treaties need to be considered in full, some provisions may be of particular importance with regard to conditions and safeguards in relation to procedural powers:

- Article 5 – Right to liberty and security
- Article 6 – Right to a fair trial
- Article 7 – No punishment without law
- Article 8 – Right to respect for private and family life

  "1 Everyone has the right to respect for his private and family life, his home and his correspondence.

  2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The European Court of Human Rights has issued a series of judgments concerning directly or indirectly the Internet or information technologies.[11] A large number of judgements, while not specifically referring to the Internet or cybercrime, is related to procedural powers of law enforcement authorities, such as search and seizure or interception of communications.[12] This case law provides further guidance as to the principles to be respected.

[10] See ETS 005, ETS N°s 005, 009, 046, 114, 117 and 177 at www.conventions.coe.int

[11] See report by the Research Division of the European Court of Human Rights on "Internet: la jurisprudence de la CEDH" of 2011.

[12] As a search of the database of the Court will show.
Http://cmiskp.echr.coe.int/tkp197/search.asp?sessionid=78598907&skin=hudoc-en

Many judgments are related to article 8 (respect for private and family life). The primary objective of this article is to protect the individual against arbitrary interference by public authorities. This covers the protection of personal data[13] which is of fundamental importance, as well as the privacy of mail, telephone, email and other forms of communication. It may cover also elements related to right of a person to his or her image,[14] the recording of a voice for analysis,[15] or observation via GPS,[16] or the risk of a "chilling effect" of legal provisions on the rights of individuals.[17]

The European Convention on Human Rights and related case law:

- help protect individuals against arbitrary interference in their rights by public authorities
- help States balance or reconcile differing interests
- underline the positive obligation by States to protect the rights of individuals. This may include criminal law and law enforcement measures.

K.U. v. Finland, no. 2872/02, 2 December 2008[18]

The case is K.U. v. Finland is illustrative with regard to these points and in that it refers to the Budapest Convention on Cybercrime, in particular its procedural law provisions (paras 22 – 26).[19]

In this case, an unknown person – in March 1999 – had placed an advertisement on a dating site in the name of a 12 year old boy without his knowledge, including a picture and contact details, and offering intimate relationships. When the parents requested the police to identify the person who had placed the advertisement, the service provider refused to disclose the holder of the IP address since he was bound to confidentiality by the law in force at the time. Courts subsequently confirmed the position of the service provider. It was thus brought to the European Court of Human Rights and resulted in a judgement in December 2008.

---

[13] S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 41, 4 December 2008

[14] Sciacca v. Italy, no. 50774/99, § 29, ECHR 2005-I

Peck v. the United Kingdom, no. 44647/98, §§ 60-63, ECHR 2003-I

[15] P.G. and J.H. v. the United Kingdom, no. 44787/98, §§ 59-60, ECHR 2001-IX

[16] Uzun v. Germany (no. 35623/05, ECHR 2010-…)

[17] See relevant ECHR case law (e.g. Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=819401&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649 or Dudgeon v UK http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=Dudgeon&sessionid=81181127&skin=hudoc-en

[18] http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=843777&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649

[19] This particular case was related to obligations by Internet Service Providers. In addition to the Budapest Convention the Court referred therefore also to the following:
"27. A global conference "Cooperation against Cybercrime" held in Strasbourg on 1-2 April 2008 adopted "Guidelines for the cooperation between law enforcement and internet service providers against cybercrime." Their purpose is to help law enforcement authorities and Internet service providers structure their interaction in relation to cybercrime issues. In order to enhance cyber-security and minimise use of services for illegal purposes, it was considered essential that the two parties cooperate with each other in an efficient manner. The guidelines outline practical measures to be taken by law enforcement agencies and service providers, encouraging them to exchange information in order to strengthen their capacity to identify and combat emerging types of cybercrime. In particular, service providers were encouraged to cooperate with law enforcement agencies to help minimise the extent to which services are used for criminal activity as defined by law."

"42. The Court reiterates that, although the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (see Airey v. Ireland, judgment of 9 October 1979, Series A no. 32, § 32)."

This may include the obligation to put efficient criminal law measures in place as a deterrent against serious acts against personal data:

"43. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. There are different ways of ensuring respect for private life and the nature of the State's obligation will depend on the particular aspect of private life that is at issue. While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is, in principle, within the State's margin of appreciation, effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions (see X and Y v. the Netherlands, §§ 23-24 and 27; August v. the United Kingdom (dec.), no. 36505/02, 21 January 2003, and M.C. v. Bulgaria, no. 39272/98, § 150, ECHR 2003-XII)."

The European Court of Human Rights furthermore argued that it "is plain that both the public interest and the protection of the interests of victims of crimes committed against their physical or psychological well-being require the availability of a remedy enabling the actual offender to be identified and brought to justice" (para 47).[20]

It acknowledged that another "relevant consideration is the need to ensure that powers to control, prevent and investigate crime are exercised in a manner which fully respects the due process and other guarantees which legitimately place restraints on crime investigation and bringing offenders to justice, including the guarantees contained in Articles 8 and 10 of the Convention, guarantees which offenders themselves can rely on" (para 48). However:

"49. The Court considers that practical and effective protection of the applicant required that effective steps be taken to identify and prosecute the perpetrator, that is, the person who placed the advertisement. In the instant case such protection was not afforded. An effective investigation could never be launched because of an overriding requirement of confidentiality. Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. Without prejudice to the question whether the conduct of the person who placed the offending advertisement on the Internet can attract the protection of Articles 8 and 10, having regard to its reprehensible nature, it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context. Such framework was not however in place at the material time, with the result that Finland's positive obligation with respect to the applicant could not be discharged. This deficiency was later addressed. However, the mechanisms introduced by the Exercise of Freedom of Expression in Mass Media Act (see paragraph 21 above) came too late for the applicant.
50. The Court finds that there has been a violation of Article 8 in the present case."

Rights such as the right to private life (article 8) or the freedom of expression (Article 10) are not absolute but may be subject to conditions or restrictions as indicated in Article 8 § 2 or Article 10

[20] See Article 13 of the European Convention on Human Rights: "Right to an effective remedy".

§ 2. This points to another principle, namely, that States need to put in place a framework that allows to reconcile different interests that are to be protected.

If a State compiles, stores, uses or discloses personal information – for example in a police register – such an interference into private life must meet the conditions of Article 8 § 2, that is, be in accordance with the law, proportionate to the legitimate aims pursued and necessary in a democratic society. Where data is stored, adequate and effective guarantees against abuse by the State must exist.

Safeguards must also be put in place to supervise secret surveillance designed to protect national security in order to avoid that democracy is destroyed on the grounds of defending it.[21]

The positive obligation of States to protect individuals against violations of their private life but also of their physical or moral integrity or against criminal activities and other dangers is particularly true for vulnerable persons, in particular children and young people as seen in K.U. v. Finland. It can also apply to xenophobia, racism or discrimination or hate speech via Internet against immigrants or foreigners in order to protect public order or the rights of others.[22]

In addition to the European Convention on Human Rights (and the related case law) other instruments relevant for member States include in particular the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108).[23] A related soft law instrument is Recommendation R(87)15 regulating the use of personal data in the police sector.[24] Convention 108 is open for accession by non-member States[25] and thus entails obligations for any country that is a Party.

For countries that are not Parties to the European Convention on Human Rights, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties apply.

1.4 Principles and requirements

Article 15 of the Budapest Convention establishes – in general terms – a number of conditions and safeguards, and makes reference to international human rights standards, but refers the modalities and implementation or the specific conditions for specific investigative measures in a specific State or situation to the domestic legal and judicial system.

It is therefore not possible to determine whether a State has implemented article 15 by referring simply to one or more provisions in domestic law or by establishing a "checklist", absolute benchmarks or similar. Such an approach would be too limiting. The conditions and safeguards are subject to domestic and international jurisprudence, changing legislation, changing technology, changing crime and other factors, and thus in constant evolution. The way they are applied may depend on the specific situation and the specific investigation.

---

[21] Weber and Saravia v. Germany (dec.), no. 54934/00, § 94, ECHR 2006-XI; and Liberty and Others v. the United Kingdom, no. 58243/00, § 62, 1st July 2008). Klass and Others v. Germany, 6 September 1978, §§ 49-50, Series A no. 28).

[22] Féret c. Belgique, n° 15615/07, 16 juillet 2009, CEDH 2009

Erbakan c. Turquie, no 59405/00, 6 juillet 2006

Jersild c. Danemark, 23 septembre 1994, § 30, série A no 298

Gündüz c. Turquie, no 35071/97, § 40, CEDH 2003-XI

[23] http://www.conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=17/09/2011&CL=ENG

[24] https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1894438&SecMode=1&DocId=694350&Usage=2

[25] In August 2011, Uruguay was the first non-member State that had applied and been invited.

In general terms, one would expect a State to meet rule of law requirements[26] such as:

- There shall be no punishment without a law[27]
- Everyone has the right to a fair trial, including the presumption of innocence[28]
- Interference in the rights of individuals can only be in accordance with the law and as is necessary in the public interest – including crime prevention – or the protection of the rights of others.[29] This means that investigative measures – in particular if they entail an intrusion into rights – are to be prescribed by law.[30]
- Anyone whose rights are violated must have the right to an effective remedy[31]
- States need to put in place a framework that allows to reconcile different interests that are to be protected.
- States have a positive obligation to protect the rights of individuals. This may include criminal law and effective enforcement to bring offenders to justice.[32]

With regard to the procedural powers foreseen in the Budapest Convention the following requirements and principles are to be met:

- Principle of proportionality, meaning in particular that "the power or procedure shall be proportional to the nature and circumstances of the offence".[33] For example, particularly intrusive measures, such as interception, are to be limited to serious offences
- Judicial or other independent supervision
- Grounds justifying the application of the power or procedure and the limitation on the scope or the duration

---

[26] This simplified list is not meant to limit or reinterpret the comprehensive frameworks provided by the European Convention on Human Rights and relevant case law, or of other international human rights treaties. Consideration would also need to be given to substantive human rights requirements – in particular the freedom of expression (Article 10 of the European Convention on Human Rights) – which set limits to law enforcement.

[27] As defined, for example, in Article 7 of the European Convention of Human Rights or Article 15 of the International Covenant on Civil and Political Rights

[28] See Article 6 of the European Convention on Human Rights or Article 14 of the International Covenant on Civil and Political Rights

[29] See for example Article 8 of the European Convention of Human rights:

"1 Everyone has the right to respect for his private and family life, his home and his correspondence.

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[30] Certain conditions are to be met in this respect. For example, when drafting provisions on secret surveillance consideration is to be given to avoid interference with the right to respect for private life and correspondence. Such measures should not only be based on law but should also be accessible to the person concerned, who must moreover be able to foresee its consequences for him or her. In the European context, the case law of the European Court of Human Rights, with respect to Article 8 ("1. Everyone has the right to respect for his private ... life ... and his correspondence) shows that national laws on secret surveillance need to be rather detailed, and the requirements are even more demanding when it comes to the monitoring of lawyers and their offices. See, for example, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria
http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=819401&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649

[31] See Article 13 of the European Convention of Human Rights

[32] See for example, K.U. v. Finland

[33] See paragraph 146 of the Explanatory Report

- Powers and procedures must be reasonable and "consider the impact on the rights, responsibilities and legitimate interests of third parties".[34]

Obviously, full implementation of the Budapest Convention, including Article 15, will help countries meet rule of law principles in that it requires States to define by law which conduct is to constitute a criminal offence as well as the procedural powers of law enforcement. It helps States meet their positive obligation to protect the rights of individuals against criminal intrusion

When considering, how States implement these principles and requirements, for practical purposes, an assessment of Article 15 could comprise the following:

1. An inventory of international human rights treaties to which a State is party to

2. An overview of how the above requirements are reflected in the constitution of a State

3. An analysis of how the above requirements are reflected in the criminal law of a State in general

4. A more specific analysis of how these requirements apply when the measures of Articles 16 (expedited preservation) to 21 (interception) are applied at the domestic level.

When carrying out an assessment along these lines, it must be understood, that accession to and implementation of the Budapest Convention is a dynamic process. This process may involve technical assistance and capacity building programmes that not only support governments in the strengthening of legislation in line with the Budapest Convention but that may also engage governments and other stakeholders in a dialogue in view of strengthening safeguards and conditions.

This is the purpose of the present report, namely to promote dialogue and capacity building aimed at the implementation of Article 15.

The following contributions by Henrik Kaspersen and Joseph Schwerha show how the conditions and safeguards are applied in the Netherlands and the United States of America.

[34] Article 15 (3) Budapest Convention

2 Henrik Kaspersen:[35] Procedural powers, safeguards and conditions in the Netherlands

2.1 Introduction to Article 15

2.1.1 Meaning and purpose

Articles 14 to 21 of the Budapest Convention cover procedural law. The overall purpose of this section of the Convention on Cybercrime is to provide for harmonised legal standards to be implemented into domestic law. These standards aim to provide for an adequate level of criminalization and for adequate investigative powers, for domestic use in the first place but at the same time to enable international co-operation.

When negotiating and drafting substantive law provisions, it had to be taken into account, that (potential) Parties would maintain different principles, doctrines and legislative techniques when implementing the provisions of the Convention. For that reason, no definitions were included in the text of the Convention of notions generally applied in domestic criminal law, represented in the text of the Convention by the notions *without right* or *intent*.

The Explanatory Report contains considerations on those issues that are of a non-binding nature. At some points in the provisions, additions or declarations were foreseen that would enable a full implementation (e.g. in some cases the element *dishonest intent,* without further common definition or explanation). The Convention does not have the ambition - and cannot have the ambition – to aim at harmonisation of underlying principles, doctrine and legislative techniques of criminal law. The purposes of the Convention are fulfilled if it provides for an adequate level of harmonisation of substantive cybercrime law amongst it Parties enabling international co-operation.

Implementation of (new) legal powers into domestic procedural law - the purposes for which as well as the circumstances under which they can be applied - should be in line with the (legal) principles of domestic criminal procedural law of the implementing Party. Criminal procedural law is the necessary chain between a criminal act and the indictment of a criminal sanction by the court. Criminal procedural law thereto attributes powers to authorities for the purpose of

[35] Professor emeritus Dr. Henrik W.K. Kaspersen obtained his law degree at Utrecht University after a career as computer scientist. From 1991 he was director of the Computer/Law Institute of the Vrije Universiteit in Amsterdam, the Netherlands. In March 2010 he retired.
Cybercrime is and was one of his main subjects of scientific expertise. He participated in the drafting of the Dutch Computer Crime Act 1993. Between 1995 and 2003 he chaired, on behalf of the Dutch Government three Council of Europe expert committees that prepared the Recommendation on procedural law concerning investigation of Cyber Crime R (95) 13, the Cyber Crime Convention (CETS 185) and its Protocol on Xenophobia and Racism (CETS 189). He also chaired the Cybercrime Convention Committee (T-CY), set-up by the Parties to the Convention in order to discuss issues of application and further development. Under the Cybercrime Project of the Council of Europe he participates in projects other activities in view of global propagation of the Cyber Crime Convention.
In the Netherlands, Prof. Kaspersen advised the Minister of Justice about the implementation of the Cybercrime Convention into Dutch law.
Today, Prof Kaspersen chairs the advisory board of the Internet Watchdog foundation against racist and discriminatory expressions on the Internet.
Prof. Dr. Kaspersen chaired the editorial board of the Dutch legal journal 'Computerrecht' for nearly fourteen years and today he is still active as a member of the board. He is a member of the editorial board of the Dutch specialist journal 'Privacy and Informatie'.

application of criminal law to the culprit. At the same time it should prevent application of criminal law to innocent persons. For that reason the attribution of powers to authorities involved in the chain of criminal proceedings is not unrestricted. The purpose of such restrictions is the prevention of arbitrariness from the side of the State in relation with its individual citizens. Most States have regulated the relation between the State and its citizens in their Constitution, or on the basis of case law.

There should be a balance between the interest of criminal proceedings – and the interests of the defendant and other persons concerned. In order to achieve a just balance not only the scope of the attributed power within its restrictions is relevant, but also the way in which and the modalities under which those powers are applied by the responsible authorities. Their mandate is also to achieve a reasonable, decent, and civilized application for the purposes of criminal proceedings.

In most countries such a mandate may not specifically be expressed by the text of the legal provisions of the criminal procedural code. The manner in which criminal proceedings are conducted may as well be subject to legal principles, not explicitly expressed in the relevant legal provisions. It is in particular left to domestic courts to control the course of criminal proceedings, including the course of the preceding criminal investigations. See if those powers are not executed beyond its legal limits but also if the principles of application – such as reasonable, decent, and civilized – are met.

Given the different background and different underlying principles of criminal law and criminal procedural law of (potential) Parties to the Cybercrime Convention, it was not feasible to draft legislation that by itself would correspond with the system and principles of criminal procedural law of each (potential) Party to the Convention. Because of the divergences of domestic law, specific regulation would possibly prevent Parties from adequate implementation of the procedural powers of the Convention. The alternative would be not to address the issue in the Convention. Given the intrusive and sensitive nature of some of the new powers, this was not esteemed desirable. Article 15 Convention on Cybercrime makes clear that the coercive powers defined by the Convention should be subject of certain restrictions and limitations of application.

2.1.2 Article 15 explained

The basic function of Article 15 is that it requires implementing Parties to apply conditions and safeguards to the powers of the Convention to the same extent or in a similar way as already represented by their existing domestic criminal procedural law. In the definitions and in the terminology of the powers a clear reference is made to the traditional power of search and seizure (Articles 18 and 19) and to possible existing provisions concerning interception of telecommunications (Article 20 and 21). Parties should take inspiration from what they already have. They should also consider applying new or other conditions and safeguards depending on the nature of the power that they implement.

Article 15 paragraph 1 offers some guidance in this exercise. It presupposes that general principles to be applied in criminal procedural law are to be deducted from relevant international treaties. Although these instruments seem to cover the same or similar topics, they have a different meaning and impact. European States are Party to the Convention for the Protection of Human Rights and Fundamental Freedoms. The European Court of Human Rights in Strasbourg, by means of its case law a strong, specific and dynamic influence on law-making and the application of procedural criminal law of the Member States. It would go too far to consider the scope, content and merits of the European Convention of Human Rights in the present report. It suffices here to mention that under the Convention, in particular its Article 6, so-called principles of due process were developed which are implemented or applied by the Parties to that Convention and which have a strong influence on conditions and safeguards applied in the domain of criminal procedural law as well.

Article 15 Convention on Cybercrime does not require that Parties that are non-member States of the Council of Europe adopt and apply principles and rules as developed under the European Convention of Human Rights. For that reason reference is made to other treaties and conventions that have a strong influence on the law of its Parties, in particular where individual rights of citizens are defined. Part III of the 1966 Covenant on Civil and Political Rights contains important human rights which may have impact on the way the domestic criminal procedural law is structured. Some of these provisions directly relate to court proceedings (prohibition of torture, prohibition of self-incrimination, prohibition of discrimination, presumption of innocence). Others define individual rights such as freedom of speech or freedom of association. No provisions are included that should have to be directly applied in the domain of criminal procedural law. However, the whole set of human rights establishes a framework to which also national criminal procedural law must respond, where the rights of the defendant are concerned, as well as where the rights of other persons are affected.

A similar appreciation could be given to the 1981 Charter on Human Rights and Peoples' Rights. Article 15 does not create a hierarchy between international instruments. It could even be imagined that a (potential) Party to the Convention on Cybercrime derives its principles of criminal procedure from criminal procedural law of other countries, which in turn may have taken inspiration – or not – from one of the instruments mentioned.

The way individual States – and the courts of these States – shape the rights and guarantees for their citizens, including if they are concerned in a criminal investigation, is subject to national preferences. If there were to be a minimum requirement for a State to accede to the Convention on Cybercrime, it would be the application of the Rule of Law, meaning that the acts of the State should be based on law and not arbitrary.

In addition, Article 15 does not only make reference to international agreements but provides for further guidance when implementing the procedural law articles. In its subsections, Article 15 refers to specific conditions and safeguards to apply in relation with the powers of Articles 16-21, if necessary in addition to conditions and safeguards already implemented in domestic criminal procedural law. The conditions and safeguards are not meant to be exhaustive: Parties may always go beyond the obligations of the Convention.

In paragraph 1 of Article 15 the principle of proportionality is mentioned. Paragraph 146 of the Explanatory Memorandum shows how the principle should be understood and how it can be applied.

Paragraph 2 contains another minimum level by specifying the most common conditions and safeguards, to be found in domestic criminal procedural law, such as judicial (or other independent) supervision, grounds justifying application, limitation of scope and duration. As paragraph 147 of the Explanatory Memorandum says, the specific conditions and safeguards to be implemented depend on the intrusiveness of the legal power. Particular circumstances under which a power can be applied may require different conditions and safeguards.

Paragraph 3 refers to the impact of coercive powers on third parties, in particular if these are not involved in the commission of the crime. The interest of these persons should be balanced against the interest of criminal proceedings. Paragraph 148 of the Explanatory Memorandum in particular refers to internet service providers who have a special and intense role in the providing of information to law enforcement. Financial compensation could be part of such conditions and safeguards.

2.1.3 Summary

Article 15 of the Convention on Cybercrime in principle refers to existing conditions and safeguards under domestic criminal procedural law. A minimum requirement would be that the acceding State applies the rule of law. European Parties take guidance from the European Convention of Human Rights and the case law of the European Court of Human Rights. Other Parties may take guidance from conventions such as those mentioned in Article 15 paragraph 1 and the Explanatory Report. Such conventions do not contain specific conditions and safeguards regarding articles 16-21 of the Convention on Cybercrime but only general principles.

Therefore, article 15 sets the minimum by provides guidance for the type of conditions and safeguards to apply, by referring to the principle of proportionality (paragraph 1, see interpretation in paragraph 146), to usual conditions and safeguards such as judicial supervision, grounds, limitation of scope and time (paragraph 2 and paragraph 147 Explanatory Memorandum) and to the principle of reasonableness (paragraph 3 of article 15, and paragraph 148 Explanatory Memorandum).

2.2 Criminal Procedural Law of the Netherlands[36]

In 1926 the legislator fully reviewed the Code of Criminal Procedural Law (hereafter Criminal Procedure Law), which replaced the Dutch version of the French Code d'Instruction criminelle, in force since 1838. The new code reflected the societal debate on rights for the defendant and openness. In the course of time, several restrictions were enacted concerning cases where the interest of criminal proceedings was considered to justify a certain restriction of the rights of the defence. However, as a general safeguard, during the 70s the dogma of the exclusionary rule was developed. If evidentiary material has been obtained in violation of criminal procedural law, the court may decide not to consider this material. For that reason, the way a criminal investigation has been executed, has become an important point of discussion in court proceedings.

In addition, violation of principles of due process as a representation of the principle of equality of arms, derived from case law on Article 6 ECHR, may lead to a decision by the court to dismiss the case. Both dogma's are based upon case law and not implemented in the Code of Criminal Procedural Law. The provisions of the ECHR – where appropriate – may be directly invoked before Dutch Court (Article 93 Constitution). Another principle, derived from ECHR's case law is the principle of immediateness. Nevertheless, in Dutch criminal proceedings a documentary character has been maintained.

In Dutch Criminal Procedural Law an important place was taken by the Investigating Judge. The law mandated him with the application of intrusive investigative powers. If the Prosecution Officer had a need for application of such powers a special procedure had to be opened. Under that procedure, also the defendant had certain rights. The workload of criminal cases induced a need for simplification of the whole criminal proceedings. The Act of May 27, 1999 (Official Journal 1999, 243, in force February 1, 2000) resulted in a shift of powers between the Investigating Judge and the Prosecution Officer. The law precisely defines in which cases the Prosecution Officer

[36] The following sections contain a description of some articles of the Criminal Procedural Code of the Netherlands. No references are made to documentary sources since those sources are in Dutch only. The main texts are taken from standard works on the Criminal Procedural Code. For the same reason no references to case law are included. A complete overview of the Criminal Procedural Code is not intended here. Instead of giving a description of what the content of the relating articles is, the provisions have been translated into English. In order to avoid confusion, regulations and exemptions that are too specific have been left out. After all, this overview is to demonstrate that the application of conditions and safeguards that are already part of classical Dutch Procedural Criminal Law are also applied in the area of the collection of electronic evidence or specifically developed and applied for that area.

is authorized to act on his own, when he needs a mandate of the Investigating Judge and in which cases only the Investigating Judge is authorized.

Another important principle implemented in Dutch Criminal Procedural Law with the Act of May 27, 1999 (Official Journal 1999, 245, in force February 1, 2000) is that investigative powers and techniques shall be explicitly regulated by law. No other measures against the will of the persons involved may be executed if it would interfere with their constitutional rights. Since then the law not only concerns powers like systematic observation, infiltration and recording of confidential communications, but also extends to the phase preceding the classical criminal investigation. In the latter case, there must be, on the basis of facts or circumstances, a reasonable suspicion that someone's has committed a crime. The law enables to collect information possibly in violation of any person's constitutional right of respect of privacy. Some of the powers defined by Criminal Procedural Law are applicable during the investigation phase as well – under certain conditions – in the pre-stage. This may be the case for a number of the powers defined by the Cybercrime Convention. A number of those powers may also be applied – but under different conditions - in case of conspiracy and commission of terrorist crimes (article 126o ff Criminal Procedure Law). In order to avoid confusion, only the law concerning the classical criminal investigation will be discussed hereafter.

In this context should also be mentioned the principle of subsidiarity and proportionality. Law enforcement authorities shall reasonably weigh the relevant interests of the persons concerned. If more than one method is available to achieve the purposes of a criminal investigation, the less intrusive or less burdensome for the defendant or other persons concerned should be applied.

2.3 Gathering electronic evidence

2.3.1 Structure of coercive powers

Article 148 paragraph 1 Criminal Procedure Law makes the Prosecution Officer accountable for the investigation of crimes, committed within the jurisdiction of the court of first instance to which he is connected.

If the Prosecution Officer deems it necessary to involve the Investigating Judge he requires the opening of a preliminary investigation, in which the Investigating Judge is leading and active. In some cases, when the facts are not fully known, the investigating judge may hear witnesses, experts and the suspect, under maintaining of the rights of the defence. The investigation by the Investigating Judge is independent and is supposed to be more neutral than carries out by the Prosecution Officer. A preliminary investigation by the Investigating Judge does not exclude continuation by the Prosecution Officer of the criminal investigation. They may be run in parallel. In order to carry out a preliminary investigation, the Investigating Judge is entitled to order the showing of the suspect, witnesses and expert and may order the preliminary detention of the suspect. He is also entitled to order the observation of the suspect and the imprisonment of non-cooperating witnesses. Furthermore, the Investigating Judge is competent to inspect a location or premises, he is entitled to seize objects, to search a location or premises, the inspection of body and cloth and the taking of bodily samples for DNA-testing, if he is investigating a case.

In other cases, the Prosecution Officer is authorized to execute the same authorities, sometimes surrounded by more restrictions, but for a number of them the Prosecution Officer needs empowerment of the Investigating Judge – which may be subject to refusal.

In some cases the Prosecution Officer may act without prior empowerment or control of the Investigating Judge.

At a lower level of competence it is the police officer who is entitled to execute certain coercive powers, either by himself or with empowerment of the Prosecution Officer.

The way these categories or cases are defined is a matter of specifying grounds and conditions for application as will be discussed hereafter.

2.3.2 Definitions

Legal definitions of the Prosecution Officer and the Investigating Judge need not to be discussed here.

The definitions of the Cybercrime Convention are, in as far as computer data and computer system are concerned, only implemented in the Code of Substantive Criminal Law. Article 80quinquies Criminal Code is literally copied from the Convention. Article 80sexies Criminal Code says that under a computer system should be understood a feature meant for the storage, processing or transfer of data – referring to article 80quinquies Criminal Code – in an electronic way.

The courts apply these definitions in the same way in the domain of Criminal Procedural Law.

The definition of service provider is included in article 1.1 Telecommunication Act. Since this concerns service providers of public communication services and networks only a dedicated definition is included in article 126la Criminal Procedure Law.

Traffic data is defined by a statutory instrument under article 13.2a Telecommunication Act.

2.3.3 Search and seizure (Articles 16-19 Cybercrime Convention)

The terminology used in the Convention, in particular in Article 19 recommends implementing Parties to draft regulation in parallel with the existing provisions on search and seizure. Under Dutch Criminal Procedural Law, an item is capable of being seized if needed for the criminal investigation (or if necessary to confiscate).

Lap-top, notebooks, i-Pods, I-pads, Blackberries or components of a computer system are tangible objects and can be seized by a police-officer. Certain restrictions – as we will see hereafter – will have to be taken into account. In case of seizure the items can be taken away for further inspection. The law does not provide for explicit authorities to inspect a computer, to use it or to make copies of the data therein (preferably by forensic experts). These authorities are supposed to be included in and covered by the power of seizure.

2.3.4 Implementation of Article 19 Convention on Cybercrime

In order to be able to inspect a computer system for the presence of data necessary for the criminal investigation, a first step is to obtain access to the location of the computer system. The law specifies who under which circumstances and on what ground is authorized to access a location for the purpose of an investigative activity.

These powers are surrounded with more restrictions depending on the function of the investigative authority: less in case of the Investigating Judge, much more in case the police officer, if authorised at all.

The search of a computer system is regulated in parallel to traditional search and seizure of tangible objects. In case of red-handed or in case of suspicion of a serious crime (see above) the Prosecution Officer may enter any place except a dwelling, without permission of the resident or an office of a person bound by a professional secrecy. (In urgent cases the assistant Prosecution Officer is authorised if empowered by the Prosecution Officer, even if given afterwards).

In other cases the Investigating Judge empowers the Prosecution Officer (on the basis of a motivated request).

Articles 125i Criminal Procedure Law ff regulate the search of premises for the purpose of safeguarding computer data, stored or recorded on a data carrier found at the premises. The same conditions and safeguards should apply as with regard the search of premises for the purpose of seizure, as regulated in articles 96 paragraph 2, 98, 99 and 99a Criminal Procedure Law.

Articles 96 paragraph 1 empowers the police officer to access any location and seize objects in case the perpetrator is caught red-handed in the commission of a serious crime (as specified by article 67, paragraph 1 Criminal Procedure Law). Article 96 paragraph 2 empowers a police officer to take measures to prevent the loss, damaging, making useless of objects that are susceptible of seizure, while waiting for the Investigating Judge or Prosecution Officer who are competent to search the location (to which the police officer is not). Article 98 Criminal Procedure Law is enacted to prevent that objects belonging to other persons would be unnecessarily seized. The person who is living at the premises has to be heard, if he is absent persons who have their domicile in the same house, including the suspect. Article 99 prohibits the seizure of documents concerning person with a professional duty of secrecy. Article 99a Criminal Procedure Law allows the suspect to be assisted by a legal counsel if it would not delay the search.

Article 125j Criminal Procedure Law implements Article 19 paragraph 2 Convention on Cybercrime.

The translated text reads:
1. In case of a search of a computer system a connected computer system present at another location may be searched for data reasonably necessary to establish the truth. If found, the data may be safeguarded (=copied).
2. This search does not extend any further than persons who regularly work or reside at the place from which the search is undertaken have access to the other system, with authorisation of the right holder.

Article 125k Criminal Procedure Law implements Article 19 paragraph 4 Convention on Cybercrime.

The translated text reads:

1. In as far as the interest of the criminal investigation clearly requires, when the power of Article 125i or 125j is applied, a person who reasonable may be expected to avail of knowledge about security of a computer system, may be ordered to provide access to the present computer systems or part of it. The person to whom the order is directed, shall if required, obey the order by providing information about the security.
2. The first section applies accordingly if in a computer system encrypted data are found. The order is directed towards the person who is reasonably being expected to avail over knowledge about the manner of encryption of that data.
3. The suspect cannot be ordered neither can a person who is legally excused not to testify (professional secrecy).

Article 125l Criminal Procedure Law is a parallel provision of Article 98 Criminal Procedure Law, concerning search and seizure of tangible objects.

The translated text reads:
1. Data that are input by or on behalf of persons with a professional duty of secrecy (public servants, notary, medics, accountants) cannot be searched if the data are object of the duty of secrecy, unless with their consent.

Article 125la Criminal Procedure Law is directed against so-called fishing operations in relation with service providers. Because of their special role as intermediary in the process of confidential communications – as protected by Article 13 Constitution – limitations are set to the search of the server of a service provider:

The translated text reads:

If during a search for the purposes of safeguarding data takes place with a service provider of a public telecommunication network or a public communication service data are found not meant for him or not originating from him, the Prosecution Officer is only authorised to determine that this data will be inspected or safeguarded if apparently forwarded by the suspect, meant for him, are related to him, have been used for the commission of the crime, or if the crime apparently has been committed to this data. The Prosecution Officer needs a preceding empowerment by the Investigating Judge, to obtain by his request.

Article 125m Criminal Procedure Law is a transposition of the general duty, in case of application of coercive measures that an official report is to be drawn up. In this case, the provisions concern the search of computer data. If relevant, the official report will be made part of the criminal (court) file.

The translated text reads:

1. If a search leads to the recording/safeguarding or making inaccessible of data (see hereafter under Article 125o Criminal Procedure Law as soon as possible a notification in writing will be made about this recording or making inaccessible as well as about the nature of the data recorded or made inaccessible.
2. The Prosecution Officer, or if the Investigating Judge has performed a search, the Investigating Judge may determine that the notification as meant in paragraph 1 to a person concerned will be postponed as long as the interest of the criminal investigation does not resist against the notification.
3. Persons concerned in the meaning of this article are:
a. The suspect;
b. The data controller;
c. The person entitled to the premises where the search took place.
4. If the suspect is the person concerned, notification need not to be given if he will be informed by inclusion of the event in the criminal file.

Article 125n Criminal Procedure Law is not inspired by the Convention but is enacted in order to protect the privacy of the persons concerned. The Act on Police Data regulates the processing of personal data by the police in other cases than during a criminal investigation (Act on Police Data 2007, in force Official Journal 2007, 549).

The translated text of article 125n reads:

1. As soon as it appears that data safeguarded during a search of premises is no longer of value for the investigation, it shall be deleted.
2. Deletion is ordered by or on behalf of the person who safeguarded the data. An official statement about the deletion is added to the criminal file.
3. The Prosecution Officer is entitled to determine that data safeguarded during a search of premises may be used for:
a) Another criminal investigation than for which purpose the power was executed;
b) Processing of data for integrity purposes (see Act on police data)
4. If paragraph 3 under a is applied, deletion of the data need not, in deviation of paragraph 1, to follow before the end of the other investigation. In paragraph 3 under b is applied, there is no

need to erase the data, until the Act on Police Data would no longer allow the storage of such data.

Article 125o Criminal Procedure Law regulates the making inaccessible of computer data, e.g. if found incidentally during a search.

The translated text reads:

1. If during a search of an automated device for the storage processing and transfer of data, data is found in relation to which or by means of which the crime is committed, the Prosecution Officer, or during a preliminary proceedings the Investigating Judge, may determine that such data will be made inaccessible in as far as necessary to end the crime or to prevent the commission of new crimes.
2. Under making inaccessible should be understood: the taking of measures in order to prevent that the operator of the aforementioned automated device or third persons take cognizance of such data of use it, or to prevent further dissemination of such data. Under making inaccessible is also to be understood the removal of such data from the automated device, under preservation of the data on behalf of criminal proceedings.
3. As soon as the interest of the criminal proceeding does no longer resist the suspension of the measures, as meant in paragraph 2, the Prosecution Officer, or during a preliminary investigation, the Investigating Judge determines that the data will be made available again to the operator of the automated device.

2.3.5 Implementation of Article 18 Convention on Cybercrime

Article 18 Convention on Cybercrime actually has two functions. Its paragraph 1a refers to the production of computer data in general, where paragraph 1b, 2 and 3 refer to subscriber information in view of the collection of traffic data and the interception of electronic communications as regulated by article 20 and 21 Convention on Cybercrime. These functions are regulated in different parts of Dutch criminal procedural law. In order to avoid confusion, the supply of traffic data and subscriber data will be discussed in the next paragraph. In this paragraph the implementation of Articles 16 and 17 Convention on Cybercrime will be considered too.

Chapter I, Title IV a, dept.8 contains the powers concerning what is called the requisition of (computer) data. While attributing powers the law takes into consideration the position of the authority in the hierarchy of the criminal investigation (Investigating Judge, Prosecution Officer, police officer) and the interest of the data concerned. It is distinguished between identifying data, other data and sensitive data. The procedure is formalised and is executed on the basis of standard written orders. The underlying principle is that if law enforcement authorities want to obtain data held by civilians, the latter have a right to know why, on what legal basis, and who is the responsible authority. As a matter of fact, this practise should replace the informal and oral collection of information.

Non-obedience in the case of an authorised requisition is a criminal act (article 184 Criminal Code).

The regulation in enacted by Article 126nc to 126ni Criminal Procedure Law.

Article 126nc Criminal Procedure Law reads in translation:

1. In case of suspicion of a crime the police officer may for the interest of the criminal investigation require from the person who reasonably qualifies and who other than for his personal interest processes data, to supply specific stored or recorded identifying data about a person.
2. Under identifying data should be understood:
   a. Name, Address, Residence;
   b. Date of birth, gender;
   c. Administrative marks;
   d. In case of a legal person, instead of the data under a. and b.: name, address, mail address, legal structure and seat.
3. A requisition as meant in paragraph 1 cannot be directed at the suspect. Article 96a paragraph 3 is to be applied similarly. The requisition cannot concern personal data concerning somebody's religion or conviction, race, political denomination, health, sexual life or membership of a union.
4. A requisition as meant in paragraph 1 is in writing and contains:
   a. A description of the person to who's identifying data the requisition is related;
   b. The identifying data that are required;
   c. The period of time within the data must be supplied and the manner in which the data must be supplied;
   d. The (legal) basis of the requisition.
5. In urgent cases the requisition as meant in paragraph 1 can be given orally. In that case the police officer puts the requisition in writing afterwards and hands it over to the person on whom the requisition was served, within a period of three days.
6. The police officer prepares an official statement of the supply of the identifying data, including
   a. The data, meant in paragraph 4;
   b. The data supplied;
   c. The crime and, if known, the name of the suspect. If not, an indication as accurate as possible of the suspect;
   d. The facts and circumstances to demonstrate that the conditions as meant in paragraph 1 are met.
7. More precise rules for daily practice in a statutory instrument.

Article 126nd Criminal Procedure Law

1. In case of suspicion of a crime as defined in article 67 paragraph 1 (serious crime) the Prosecution Officer may for the interest of the criminal investigation require from the person who reasonably is suspected to have access to certain stored or recorded data to supply this data.
2. A requisition as meant in paragraph 1 cannot be served upon the suspect. Article 96a paragraph 3 is to be applied similarly. The requisition cannot concern personal data concerning somebody's religion or conviction, race, political denomination, health, sexual life or membership of a union.
4. A requisition as meant in paragraph 1 is in writing and contains:
   a. If known, the name or otherwise an as precise indication of the person or person concerning who data are required;
   b. An accurate as possible indication of the data required and the period of time within and the manner how the data have to be supplied;
   c. The (legal) basis of the requisition.
5. In urgent cases the requisition can be given orally. In that case the Prosecution Officer puts the requisition in writing afterwards and hands it over to the person on whom the requisition was served, within a period of three days.
6. The Prosecution Officer sees that an official statement of the supply is prepared, including
   a. The data, meant in paragraph 3;
   b. The data supplied;

c. The crime and, if known, the name of the suspect. If not, an indication as accurate as possible of the suspect;

d. The facts and circumstances to demonstrate that the conditions as meant in paragraph 1 are met.

e. The reason why the data are required in the interest of the criminal investigation.

7. In case of suspicion of another crime than meant in paragraph 1. The Prosecution Officer is entitled, in the interest of the criminal investigation, to issue a requisition as meant in that paragraph. With preceding empowerment of the Investigating Judge. The Investigating Judge empowers on the request of the Prosecution Officer. Paragraph 2 to 5 are similarly applicable.

In case of the periodically processing of the same or similar data, article 126ne Criminal Procedure Law even provides for a disclosure order that refers to data, processed at the time of issuance or the requisition but also after that moment of time.

1. The Prosecution Officer is entitled to determine, in the interest of the criminal investigation, that a requisition as meant in article 126nd paragraph concerning the person who processes data other than for personal use, may relate to data that are being processed after the moment of time the requisition was served. The period of time to which the requisition applies is four a maximum of four weeks and may be subject of renewal, every time for the same period of time. The Prosecution Officer mentions this period in the requisition. Article 126nd paragraph 2-5 are similarly applicable.1 In case of suspicion of a crime as defined in article 67 paragraph 1 (serious crime) the Prosecution Officer may for the interest of the criminal investigation require from the person who reasonably is suspected to have access to certain stored or recorded data to supply this data.

2. In a case as meant in ss 1 the Prosecution Officer determines the execution of the requisition is to be finished as soon as the conditions, meant in article 126nd paragraph 1, are no longer met. The Prosecution Officer see that an official statement is made up of amendment, supplementation, extension or termination of the requisition.

3. If the interest of the criminal investigation requires it urgently, the Prosecution Officer is entitled to determine, in a case as meant in paragraph 1, that the person upon whom the requisition is served, supplies the data immediately after the processing, or every time within a specified period after the processing. The Prosecution Officer needs the preceding empowerment of the Investigating Judge to be issued at his request.

Article 126nf Criminal Procedure Law: sensitive data

1. In case of suspicion of a crime as defined in article 67 paragraph 1 (serious crime) that given its nature or the coherence with other crimes committed by the suspect, severely infringes upon the legal order, the Prosecution Officer is entitled, if the interest of the criminal investigation requires it urgently, to require from the person who reasonably is suspected to have access to data as meant in article 126nd paragraph 2, third phrase to supply this data.

2. A requisition as meant in paragraph 1 cannot be served upon the suspect. Article 96a paragraph 3 is to be applied similarly.

3. A requisition as meant in paragraph 1 can only be issued after preceding empowerment in writing, to be given by the Investigating Judge at the request of the Prosecution Officer.

4. Article 126nd, paragraph 3-5 and 7 are to be applied similarly.

Article 126ng Criminal Procedure Law regulates the supply of subscriber information by service providers. The definition of a service provider is included in article 126la Criminal Procedure Law, because for the sake of implementation of the Cybercrime Convention, the definition of a service provider should be wider than provided for in the Telecommunication Act, where only providers of public electronic communication services are considered.

Article 126la Criminal Procedure Law:
a. Provider of a communication service: natural or legal person who in the context of a profession or company offers the users of his service the possibility to communicate by means of a computer system, or processes or stores data on behalf of such service or on behalf of the users of such service.
(Note: includes public and private, includes caching, proxy-internet servers as well as hosting providers). It is wider than the definition of the Telecommunication Act.
b. User of a communication service: natural or legal person who went into a contract for the use of the service or who in fact uses the service.

Article 126ng Criminal Procedure Law does not refer to traffic data or subscriber information, but that does not mean that also a service provider could avail over data that may be relevant for criminal investigations. However, the provision is not meant to open an easier way of obtaining messages that a provider transfers on behalf of the users of its service. Therefore, the possible requisition of such data is possible but only under specific conditions and safeguards.

The translated text reads:

1. A requisition as meant in articles 126nc paragraph 1, 126nd, paragraph 1 or 126ne, paragraph 1 may be served upon a service provider in the meaning of article 126la in as far as relating to other data that may be required on the basis of articles 126n and 126na. The requisition may not concern data that are stored in the automatic device of the provider and which are not meant for him or originate from him.
2. In case of suspicion of a crime as defined in article 67 paragraph 1 (serious crime) that given its nature or the coherence with other crimes committed by the suspect, severely infringes upon the legal order, the Prosecution Officer is entitled, if the interest of the criminal investigation requires it urgently, to require from the provider who reasonably is suspected to have access to data as referred to in the last phrase of paragraph 1, to supply this data, in as far as apparently originating from the suspect, are meant for the suspect, concern the suspect or served for the commission of the crime, or if the crime was apparently committed concerning the data.
3. A requisition as meant in paragraph 1 cannot be served upon the suspect. Article 96a, paragraph 3 is to be applied similarly.
4. A requisition as meant in paragraph 1 can only be issued after preceding empowerment in writing, to be given by the Investigating Judge at the request of the Prosecution Officer.
5. Article 126nd, paragraph 3-5 and 7 are to be applied similarly.

As additional instrument, Article 126nf Criminal Procedure Law provides for a possible solution in case produced data are encrypted:

1. The Prosecution Officer is entitled, if the interest of the investigation so requires, when applying, or shortly after application of, articles 126nd, ss. 1, 126ne, paragraph 1 or 3, 126nf, paragraph 1, to order the person who reasonably can be suspected to have knowledge of the manner of encryption of the data referred to in these articles, to cooperate to the decryption of the data by undoing the encryption, or to make his knowledge available.
2. The order cannot be given to the defendant. Article 96a, paragraph 3 applies similarly.

The preservation order, included in Article 16 as well as in article 17 Convention on Cybercrime, is rather literally implemented in Article 126ni Criminal Procedure Law:

1. In case of suspicion of a crime as defined in article 67 paragraph 1 (serious crime) that given its nature or the coherence with other crimes committed by the suspect, severely infringes upon the legal order, the Prosecution Officer is entitled, if the interest of the criminal investigation requires it urgently, to require from the person who reasonably is suspected to have access to specific data that at the time of the requisition is stored in an automated device and with regard to which reasonable can be assumed that it is particularly susceptible to loss or modification, that this data be preserved and hold available for a period of maximum 90 days. The requisition cannot be served upon the suspect.
2. If the requisition is served upon a service provider in the meaning of article 126la and the requisition concerns as well data as meant in article 126n, paragraph 1 [=traffic data], the service provider is obliged as soon as possible to supply the data necessary to establish the identity of other service providers whose services he uses.
3. The requisition is served in writing or orally. If the requisition is served orally, the Prosecution Officer sees that the requisition is put in writing as soon as possible and that a certified copy is handed over to the person to whom the requisition applies. With serving the requisition and when putting is writing is mentioned:
    a. An as accurate description of the data to be held available;
    b. The moment of time of the requisition;
    c. The (legal) basis of the requisition;
    d. The period of time that the data shall be held available, and
    e. If ss. 2 is applicable.
4. The Prosecution Officer sees that an official statement is made up of the requisition and, if it was done orally, of the putting in writing, containing:
    a. The data meant in paragraph 3;
    b. The crime and, if known, the name of the suspect. If not, an indication as accurate as possible of the suspect; and
    c. The facts and circumstances to demonstrate that the conditions as meant in paragraph 1 are met.
5. The requisition is one time subject to renewal for a maximum period of 90 days. Ss. 2, 3, 4 shall be similarly applied.

The provisions on the requisition of data were recently evaluated. The main findings of the report[37] are:

1. The powers of the Act are frequently applied. Mainly the powers are used to obtain data for identification purposes and historical data [in contrast with 'future data', i.e. data that most likely will be processed or possessed by a person]. Other powers under the law are rarely applied for criminal investigations.

2. Most holders of data in general comply with requests for information submitted to them by the investigating authorities. However, banks and financial institutions raise the threshold somewhat by taking more time to deliver the information and by submitting it on paper only. Given the growing importance of financial investigations stricter requirements could be imposed on such actors.

3. There is an overlap in the definition of information and of objects carrying information. Investigating authorities therefore have to decide how the information required is made available to them. E.g. in some cases it is not necessary to hand over an original document

[37] "Fuel for the investigation, Evaluation of the Act Ordering Data, Boom- the Hague 2011". Comments by Henrik Kaspersen added in [brackets].

where a copy would suffice. It would also prevent that holders information deliver it in the format they prefer.

4. The legislator left room for interpretation about data for identification purposes and other data and sensitive data (see article 126nc Sv and article 126nd Sv). On the matter was ruled by the Supreme Court in its Trans Link decision. The legislator did not take into account the case that investigating authorities request for non-sensitive information but nevertheless receive information that according to the law can be qualified as sensitive data. A solution could be to lower the level of application of the power to order the production of CCTV (Camera Observation Images) recorded in public places).

5. The competence to order the production of identification data should be restricted to police officers who act as assistant to the public prosecutor [and not to any police officer]. Those officers should be trained in order to be able to adequately assess the nature of specific requests.

6. Criminals could misuse parties who are exempt from obligations to comply with production orders for data. A detailed legal review should precede solution of this problem.

2.3.6 Service Providers and e-communications

The Netherlands has implemented the European Directive on Data Retention. The retention period is twelve months. The legal system around the collection of traffic data and interception of e-communications is as follows. Chapter 13 of the Telecommunication Act regulates the obligations of providers of public electronic communication networks and public communication services in relation with law enforcement authorities and the secret services.

A service provider is only entitled to only offer his services to the public if the traffic transmitted over his communication systems can be intercepted on behalf of law enforcement and the secret services (see hereafter). Apart from interception of content, service providers are obliged to preserve so-called traffic data and location data (cell phone) for a period of 12 months (article 13.2a Telecommunication Act). What has to be understood under traffic data is defined in an appendix to the Telecommunication Act. Article 13.2b Telecommunication Act stipulates that service providers have to produce such data if ordered by law enforcement authorities on the basis of the relevant provisions of the Criminal Procedural Code.

Article 13.4 obliges service providers to produce traffic data, if ordered by law enforcement or secret services. The main provision is here Article 126n Criminal Procedure Law.

The translated text reads:

1. In case of a suspicion of a crime as defined in article 67 paragraph 1, the Prosecution Officer is entitled in the interest of the investigation to require to supply data about the user of a communication service and the communication traffic concerning this user. The requisition shall only concern data defined by statutory instrument and may concern data which:
   a. Are processed at the moment of time of the requisition;
   b. Be processed after that moment.
2. The requisition, meant in paragraph 1, can be served upon every provider of a communication service. Article 96a, paragraph 3, applies similarly.
3. If the requisition concerns data meant in paragraph 1, second phrase, under b, the requisition is done for a maximum period of three month.
4. The Prosecution Officer sees that of the requisition an official statement is made up, which includes:
   a. The crime and, if known, the name of the suspect. If not, an indication as accurate as possible of the suspect;

b. The facts and circumstances to demonstrate that the conditions as meant in paragraph 1 are met.

c. If known, the name or otherwise, as accurate as possible, an indication of the person about whom data are required;

d. The required data;

e. If the requisition concerns data as meant in paragraph 1, second phrase, under b, the period the requisition was foreseen for.

5. If the requisition concerns data as meant in paragraph 1, second phrase, under b, the requisition is to be ended as soon as the conditions, meant in paragraph 1, first phrase, are no longer met. The Prosecution Officer sees that an official statement is made up of amendment, supplementation, prolongation, or ending of the requisition.

6. A Statutory Instrument may provide for regulation for the Prosecution Officer to require data.

Above, for the implementation of article 18 paragraph 1b Convention on Cybercrime ff it was referred to this paragraph. Article 126na Criminal Procedure Law concerns the implementation of user (subscriber) data. Subscriber data are defined in the Statutory Instrument on the production of data telecommunication (Official Journal 2000, 71). It is not the place here to discuss items under the notion of traffic data.

The translated text of article 126na Criminal Procedure Law reads:

1. In case of a suspicion of a crime the police officer is entitled in the interest of the investigation to require to supply of data concerning name, address, ZIP-code, domicile, [telephone] number and type of service of a user of a communication service. Article 126n, paragraph 2, is applicable in a similar matter.

2. If the data, meant in ss. 1 are not known by the service provider and if the data is needed for the application of article 126m [interception] or article 126n the Prosecution Officer may, in the interest of the investigation require that the provider reproduces and supplies the data according to the procedure specified in a Statutory instrument.

3. […]

4. A Statutory Instrument may provide for regulation how the Prosecution Officer or the police officer requires data.

Article 126m Criminal Procedure Law is the main article concerning the interception of e-communications. Because of the difference between the definition of a service provider in the Telecommunication Act and the one in article 126la Sv, article 126m deals with interception without co-operation of the service provider not under the Telecommunication Act as well as co-operation of the provider on the basis of the Telecommunication Act. This is not the place to discuss the technical measures that enable the interception of communication.

The translated text reads:

1. In case of suspicion of a crime as defined by article 67 paragraph 1 (serious crime) that given its nature or the coherence with other crimes committed by the suspect, severely infringes upon the legal order, the Prosecution Officer is entitled, if the interest of the criminal investigation requires it urgently, to order a police officer that a communication not meant for the public by using the services of a provider of a communication service (see article 126la] is recorded by technical means.

2. The order is in writing and specifies:

a. The crime and if known the name of otherwise an as accurate indication of the suspect;

b. The facts and circumstances that demonstrate that the conditions of paragraph 1 have been met;

c. If possible, the number or other indication by which the individual user of the communication service is identified, as well as, if known, the name and address of the user;

d. The period of time that the order is valid;

c. An indication of the nature of the technical means by which the communication is recorded.

3. If the order concerns a communication that takes place over a public communication network or by using a public communication service as defined in the Telecommunication Act, the order is executed with cooperation of provider of the public communication network or the public communication service, unless it is not possible or if the interest of the investigation would oppose it. In that case the order is accompanied by the requisition of the Prosecution Officer to cooperate.

4. If the order concerns other communications than meant in paragraph 3, the provider is given the opportunity to co-operate in the execution of the order, unless impossible or if the interest of the investigation would oppose it.

5. The order, as meant in paragraph 1, can only be issued after empowerment in writing, to be given by the Investigating Judge after request of the Prosecution Officer. Article 126l paragraph 5-8 applies similarly.

6. Where the interest of the investigation would clearly require it, in case of application of paragraph 1, the person, who can reasonably be suspected to have knowledge of the manner of encryption of the communication, can be required to co-operate to decrypt the data, either by making available the knowledge, or by decrypting the data.

7. The requisition meant in paragraph 6 is not served upon the suspect.

8. Article 96a, paragraph 3, and article 126l, paragraph 4, 6 and 7 apply similarly to the requisition meant in paragraph 6.

9. A Statutory Instrument may provide for regulation about the manner the order of paragraph 1 and the requisitions of paragraph 3 and 6 are served and how these can be obeyed.

2.4 Other legal safeguards

Separately, a number of other legal safeguard should be mentioned here, Dutch Criminal Law does not provide for an appeal by the defendant against the execution of the coercive powers dealt with above. It is up to the trial judge to see if the execution of coercive powers has been within the limits of the law. If not, evidence obtained in violation of the law may be excluded by the court.

In cases where the law proscribes that the Prosecution Officer needs the empowerment of the Investigating Judge, the latter may refuse to give his permission. If necessary, the decision is in writing and motivated.

One specific provision has to be mentioned:

Article 552a enables interested persons to file a written complaint about the seizure and handling of tangible objects. The chambers of the court deal with these complaints in a public session and take decisions. The court only decides to measures. It does not provide for financial compensation. In parallel with seizure of tangibles the procedure is open for the following as well:

1. […] about the requisition of data, the requisition to provide co-operation concerning the decryption of data, the taking cognizance or use of data that were safeguarded during a search or supplied on the basis of a requisition, the taking cognizance or use of data stored, processed or transmitted by means of an automated device and recorded during the search of such a device, […] the requisition to preserve data and hold it available, about the making inaccessible of data , found in an automated device […]

2. The interested persons are entitled to request in writing the erasure of data that were safeguarded during a search or supplied after a requisition.

3 Joseph J. Schwerha: Article 15 from a U.S. perspective[38]

3.1 Introduction

The purpose of this article is to provide an illustration of the requirements set forth in Article 15 of the Council of Europe's Convention on Cybercrime, whilst providing explicit examples on how those requirements have been implemented in the United States. This paper is split up into three main parts. The first part describes the Convention and Article 15, in particular. The second section mainly sets forth the conditions and safeguards called for under Article 15 by describing Articles 16-21 and how the conditions and safeguards called for in those subsections are implemented within the United States. In the last section, the author provides commentary from United States scholars, academics and experts outlining the methods in which the safeguards and conditions of Article 15 could be better implemented within the United States. Given the broad scope of the safeguards and conditions called for under section two of the Convention on Cybercrime, this article does not seek to provide a comprehensive analysis, but rather sets forth a more general evaluation, only illustrating specifics when appropriate and possible.

3.2 Background

3.2.1 Context

On 1 January 2007, the Council of Europe's Convention on Cybercrime (hereinafter referred to as the "Convention"), went into full force for the United States, thereby completing the adoption of the principles and procedures called for therein when it was originally opened for signature on 23 November 2001. While the Convention was transformative, the United States was already far along in meeting the requirements for compliance. Many would say, in fact, that the United States had to do very little, if any, modifications to its domestic laws in order to comply with the provisions of the Convention.

This article discusses the conditions and safeguards called for under Article 15 of the Convention, especially as they have been implemented in the United States. Upon ratification of the treaty, the United States arguably already had many of the provisions within its legal system since signing in November of 2001. However, U.S. compliance with the dictates of Article 15 can be found only by looking at wide and varied parts of the United States legal system. While the United States does provide for conditions and safeguards as called for by Article 15, one must really look beyond pure criminal procedure to see how these conditions and safeguards are implemented in practice. For instance, while the preservation requirement of Article 16 is clearly contained within 18 U.S.C. §2703(f) of the Stored Communications Act, the analysis does not stop there. One must continue to look to corresponding state legislation and jurisprudence that operate to similar ends, as well as other statutes that serve to protect the privacy of certain types of information.[39]

This paper is divided into several sections. In essence, however, it is split up into three main parts. The first part provides a brief history and analysis of the Convention and Article 15. The

---

[38] Joseph J. Schwerha IV, M.S., J.D., Associate Professor of Business Law & Technology, California University of Pennsylvania, Owner & President TraceEvidence, LLC. All statements contained herein solely are the opinion of the author and not of any of his employers or affiliates.
They do not necessarily reflect official positions of the Council of Europe, the European Union or of the Parties to the treaties referred to.

[39] For instance, the *Health Insurance Portability and Accountability Act* (*HIPAA*) of 1996 (P.L.104-191), requires that a person consent before the data holder could give it to the police voluntarily and before a court order was put into place.

second section mainly sets forth the conditions and safeguards called for under Article 15 by describing Articles 16-20 and how the requirements set forth in those subsections are implemented within the United States. In the last section, the author provides commentary from United States scholars, academics and experts outlining how our privacy experts believe we could better protect the civil liberties of the contract holders in the future.

3.2.2 Current U.S. Status

The protections for civil liberties in the United States derives from a combination of protections set forth in the United States Constitution, State Constitutions, Federal Statutes, State Statutes and relevant case law. While it is beyond the scope of this article to discuss every protection, the author attempts to discuss the particular statutory and case law citations when most appropriate.[40]

The procedural law section of the Convention is made up of Articles fourteen through twenty one.[41] Consequently, the topics covered in those articles are self-evident from the titles themselves:

- "Article 14 – Scope of procedural provisions";
- "Article 15 – Conditions and safeguards";
- "Article 16 – Expedited preservation of stored computer data";
- "Article 17 – Expedited preservation and partial disclosure of traffic data";
- "Article 18 – Production order";
- "Article 19 – Search and seizure of stored computer data";
- "Article 20 – Real-time collection of traffic data"; and
- "Article 21 – Interception of content data".[42]

This article is particularly concerned with the United States perspective on the conditions and safeguards set forth in Article 15.

Article 15 is a subsection of Section 2 of the Convention. It is comprised of three paragraphs, each one addressing a different aspect of how the governmental powers provided by the Convention shall be limited by "conditions and safeguards provided under its domestic law, which shall provide for the adequate protection of human rights and liberties."[43] The entire article is set forth as follows:

> "Article 15 – Conditions and safeguards
> Each Party shall 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 under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

[40] It should be noted that scores of authors have written thousands of pages on United States criminal procedure and constitutional protection of civil liberties. The scope of this article is merely to illustrate the most evident implementation of the safeguards and conditions called for in Article 15 of the Convention.

[41] See COE Convention on Cybercrime, infra at Sec. 2

[42] Id.

[43] See Art. 15 (1) of the COE Convention on Cybercrime.

> Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.[44]"

Paragraph one primarily mandates that each Party shall incorporate "conditions and safeguards" that are sufficient to ensure the "adequate protection of human rights and liberties." Further, paragraph one states that any such conditions or safeguards "shall incorporate the principal of proportionality".[45] The clause is inclusive but not limiting, in that it defines those human rights and liberties as including two specific instruments: 1. The 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, and 2. The 1966 United Nations International Covenant on Civil and Political Rights[46], as well other "applicable international human rights instruments".[47] While Article 15 does not define the human rights and liberties provided by such documents, the Preamble to the Convention mentions that those documents "reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning respect for privacy."[48]

Paragraph two attempts to identify various forms of "conditions and safeguards" that the Convention deems mandatory.[49] It states that said conditions and safeguards "shall"[50], include at least three things: 1. "judicial or other independent supervision", 2. "grounds justifying application", and 3. that such "power or procedure" shall be limited in "scope" and "duration".[51] It should be noted, however, that said limitations must also be "appropriate in view of the nature of the procedure or power concerned".[52]

Paragraph three concerns itself with a very particular issue: how the powers and procedures provided for in the procedural law section will impact the "responsibilities and legitimate interests of third parties".[53] Such concern must only be present, however, when it is "consistent with the public interest", and which further goes on to define "public interest"[54] as specifically including "the sound administration of justice."[55] Article 15 went under many revisions, as did several other parts of the Convention. Thus, in determining exactly what the Drafters meant, it is helpful to review the history of Article 15.

---

[44] Id.

[45] Id.

[46] The protections set forth by these two instruments will be discussed later herein.

[47] Id.

[48] See Preamble to Council of Europe Convention on Cybercrime (signed 23 Nov. 2001) ETS 185.

[49] Council of Europe Convention on Cybercrime (ETS 185), Article 15(2).

[50] Id.

[51] Id.

[52] Id.

[53] See Council of Europe Convention on Cybercrime (ETS 185), Article 15(3).

[54] Id.

[55] Id.

3.2.3 History and Background of the Budapest Convention

The history of the Convention is well known.[56] After four years and twenty-seven drafts[57], the forty-one nation Council of Europe adopted the Convention on Cybercrime through the Committee of Ministers during the Committee's 109th Session on 8 November 2001.[58] The Convention was opened for signature in Budapest, on 23 November 2001, during which 30 countries signed the Convention (including four non-members of the Council of Europe, that is, Canada, United States, Japan and South Africa that participated in the negotiations).[59] By September 2011, 47 States have signed and 32 States have ratified the Convention on Cybercrime.[60]

The Convention is the first international treaty on crimes committed via the Internet and other computer networks. Its provisions particularly deal with infringements of copyrights, computer-related fraud, child pornography, and violations of network security.[61] Its main objective, set out in the preamble, is to "pursue . . . a common criminal policy aimed at the protection of society against cybercrime . . . especially by adopting appropriate legislation and fostering international co-operation."[62]

---

[56] While not the focus of this article, it is helpful to review the background of the Convention. In 1989, the Council of Europe's Committee of Ministers adopted Recommendation No. R. (89) 9 stating that Member States need to consider computer-related crime when reviewing national legislation. The Recommendation also listed implementation guidelines for legislators that would criminalize certain criminal acts.. Recommendation No. R. (95) 13 was later adopted to provide procedures for criminal law concerning issues such as search and seizure, surveillance and international cooperation.
Despite the specific recommendations issued by the Council, no formal process had been initiated that would coordinate the laws of member European states. However, in 1997, a Committee of Experts on Crime in Cyber-Space (PC-CY) was formed to examine problems related to computer crime and to implement criminal procedures dealing with the increasingly costly and pervasive form of crime. The PC-CY was to use the previous two recommendations as a foundation for examining the growing threat of computer crime and the appropriate legal structure to implement. The Committee was charged with drafting a binding legal document that became the genus for today's cyber-crime treaty. The PC-CY's legal conclusions addressed five issues: cyber offenses through telecommunication networks, harmonization of substantive criminal law, the investigative powers of law enforcement, conflict of laws issues and questions of international cooperation
In April of 2000, a draft of the treaty was finally made available to the public as well as a press release that described the basic legal elements and philosophies behind the draft convention. The press release officially declassified the draft convention and called for "businesses and associations" to comment "before the final adoption of the text." It also stated that the Council of Europe was focusing on the harmonization and the implementation of procedural and substantive criminal law with regards to cybercrime. One of the main goals was the coordination and cooperation of international law enforcement. The U.S., Canada, South Africa and Japan were named as actively participating in the treaty negotiations.

[57] See Russell G. Smith, "Cyber Criminals on Trial" (Cambridge University Press, 2004).

[58] See Council of Europe Convention on Cybercrime (signed 23 Nov. 2001) ETS 185.

[59] Id.

[60] An additional eight countries had been invited to accede, namely Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, and Philippines. Council of Europe, Chart of Signatures and Ratifications at http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=17/09/2011&CL=ENG

[61] See Council of Europe Convention on Cybercrime (signed 23 Nov. 2001) ETS 185.

[62] Id.

3.2.4 History of Article 15

While the drafting process of the Convention on Cybercrime incorporated twenty-seven drafts overall, it was not until the nineteenth version in which the Convention was made available to the public.[63] Despite the fact that versions prior to the Convention Draft No.19 have not been released for public dissemination, the difference in content with each subsequent draft shows an increased observance to privacy safeguards and procedural conditions. The creation and evolution of Article 15 from the initial draft Convention released in April 2000 to the final draft approved in June 2001 is quite telling, as the creation of Article 15 itself can be construed as a response to the wide ranging privacy and human rights concerns present within early drafts of the Convention.[64]

Early versions of the Draft Convention did not include a separate section *o*n procedural conditions and safeguards, let alone the finalized version of Article 15 referencing the explicit protection of privacy and human rights. In the initial version, Draft Convention No. 19 did not contain an article solely addressing conditions and safeguards.[65]

The operative parts of the procedural law section of the Convention Draft No. 19 included: Article 14 – Search and Seizure of Stored Computer Data, Article 15 – Production Order, Article 16 – Expedited Preservation of data stored in a computer system, Article 17 – Expedited preservation and disclosure of traffic data, and Article 18 – Interception.[66] It is important to point out that while the nineteenth draft lacked a singular article on conditions and safeguards present in the current Convention, each Article in the procedural law section[67] contained language evoking such safeguards under national law.[68] Specifically, Articles in procedural law section each contained a subsection stating, "The powers and procedures referred to in the present Article shall be subject to conditions and safeguards as provided for under national law."[69]

At the time of release, the conditions and safeguards referred to in Convention Draft No. 19 were largely ambiguous and undefined. Despite referencing a general basis in the domestic law of each ratifying state, there was no baseline as to the goal of the required procedural conditions and safeguards. Criticism at the time warned that adoption of the Convention would ultimately lead to violation of civil and privacy rights and grant governments wholesale power to enter intrude into the lives of the populace.[70]

Through subsequent drafts of the Convention, it became apparent that language pertaining to procedural conditions and safeguards would not be buried in the boilerplate of other Articles nor left in relative ambiguity. The twenty-second draft of the Convention was released in October of 2000.[71] Convention Draft No. 22 contained the first Article devoted solely to procedural laws and, to some extent, safeguards. In Article 18 of the October 2000 Convention Draft, titled "General Provisions on domestic Procedural laws", drafters attempted to combine procedural requirements

---

[63] European Comm. on Crime Problems, Draft Convention on Cyber-Crime (Draft No. 19) of the Committee of Experts on Crime in Cyber-Space.

[64] European Comm. on Crime Problems, Draft Convention on Cyber-crime of the Committee of Experts on Crime in Cyber-Space.

[65] Draft Convention on Cyber-Crime (Draft No. 19) of the Committee of Experts on Crime in Cyber-Space.

[66] Id.

[67] Absent Article 18 – Interception, which was still under discussion during the release of Convention Draft No. 19.

[68] See Art. 14 (7), Art. 15(2), Art. 16(4), and Art. 17(2).

[69] Id.

[70] See "Cybercrime Solution Has Bugs", Wired Magazine, May 3, 2000 at http://www.wired.com/politics/law/news/2000/05/36047.

[71] European Comm. on Crime Problems, Draft Convention on Cyber-Crime (Draft No. 22) of the Committee of Experts on Crime in Cyber-Space.

of the Convention, such as search and seizure powers, data productions and preservation, and interception of electronic communications with a limiting requirement to harmonize such processes with the domestic laws of each Party.[72]

While the October 2000 draft incorporated a procedural provision with reference to generalized safeguards under domestic law, subsequent drafts of the Convention expanded upon the nature of such safeguards. In November 2000, the PC-CY released the first draft to contain an Article solely devoted to the application of conditions and safeguards on criminal investigations and proceedings concerning matters related to the Convention itself.[73] Article 14, titled "Conditions and Safeguards related to the Applications of Procedural Measures", expressly assumed the need for various safeguards and procedural conditions to protect the human rights of the citizenry in situations where a criminal investigation or proceeding is undertaken for offences established in accordance with the convention.[74]

3.2.5 Adjustments in final version of Article 15

The current iteration of Article 15 took form in the finalized Draft Convention in May 2001.[75] Compared to earlier drafts of the Convention, the protections and safeguards present in the current version of Article 15, while still broad, take a rhetorical step in the right direction in attempt to lessen ambiguity. In the finalized version of Article 15, the Convention attempted to address the complicated problem of guaranteeing civil rights protection to citizens living in different cultures and political systems.[76]

Ultimately, the drafters of the Convention concluded that it was not possible to detail all of the conditions and safeguards necessary to circumscribe each power and procedure provided for in the Convention itself. As such, Article 15 was drafted to provide "the common standards or minimum

---

[72] Convention Draft No. 22, Art. 18 Quarter – General provision on domestic Procedural Laws. Art. 18 Quarter, states: 1. Each Party shall apply the measures described in articles 14.
through 17, and 18 bis to:(a) the offences established in accordance with articles 2-11 of
this Convention; (b) other criminal offences committed by means of a computer
system ;(c) evidence in electronic form of any criminal offence.
2. Each Party may, at the time of signature, or when depositing its instruments of ratification, acceptance, approval or accession, by declaration addressed to the Secretary General of the Council of Europe, declare that it reserves its right to apply the measure referred to in Article 18 only to offences or categories of offences specified in such declaration.
3. For the purposes of Article 18, the range of serious offences covered shall be determined by the domestic law of the Party concerned.
4. The powers and procedures referred to in articles 14 through 18 shall be subject to the conditions* and safeguards provided for under the domestic law of the Party concerned.

[73] European Comm. on Crime Problems, Draft Convention on Cyber-Crime (Draft No. 24 Rev. 2) of the Committee of Experts on Crime in Cyber-Space.

[74] Draft Convention on Cyber-Crime (Draft No. 24 Rev. 2), Art. 14 - Conditions and Safeguards related to the Application of Procedural Measures. Article 14, states: 1. The measures adopted in accordance with this Section shall be applied for the purpose of criminal investigations and proceedings concerning the offences established in accordance with Articles 2 - 11 of this Convention, other criminal offences committed by means of a computer system, or the collection of electronic evidence of a criminal offence.
2. The application of the measures adopted shall be subject to the conditions and safeguards provided for under the domestic law of the Party concerned, with due regard for the adequate protection of human rights and, where applicable, the proportionality of the measure to the nature and circumstances of the offence.

[75] See Final Activity Report: Draft Convention on Cybercrime and Explanatory Memorandum Related Thereto, May 25, 2001 at http://cryptome.org/cycrime-final.htm#DRAFT%20REPORT.

[76] See Council of Europe Convention on Cybercrime (signed 23 Nov. 2001) ETS 185.
Explanatory Report at P. 144

safeguards to which Parties to the Convention must adhere."[77] The minimum safeguards referenced in Article 15 pertain to certain applicable human rights instruments including: the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms, the ECHR Additional Protocols No.1, 4, 6, 7 and 12, and the 1966 United Nations International Covenant on Civil and Political Rights.[78] Accordingly, the Convention instructs Parties to incorporate current domestic law to limit the scope of protection orders authorized, provide reasonableness requirements for searches and seizures, and minimize intrusion regarding interception measures taken with respect to the wide variety of offenses.[79]

While Article 15 provides a basis for the high level protection of human rights and personal liberty in light of the Convention, much is lacking in concern to the practical implementation of such safeguards. The Explanatory Report loosely identifies procedural safeguards "as [those] appropriate in view of the nature of the power or procedure, judicial or independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or duration thereof."[80] Specifically, the Convention instructs that "[n]ational legislatures will have 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."[81] Thus, while the Convention provides ambitious language regarding the domestic implementation of human rights instruments, the treaty offers no specific minimal procedural guarantees of due process or privacy rights in its implementation.

3.2.6 U.S. overarching safeguards and conditions in all criminal proceedings

The United States has many protections for the civil liberties of its public against unwarranted governmental intrusions. The primary protection is found in the Fourth Amendment to the United States Constitution, which reads as follows:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[82]

This is the primary instrument providing protection against inappropriate government intrusion into the lives of private individuals. In criminal proceedings, provisions of the Fourth Amendment are highlighted. Under the Fourth Amendment, the Public should be confident that, absent a warrant, or one of its exceptions no person from the government should invade their privacy. In particular, in order to avail themselves to the protections inherent in the Fourth Amendment, said person must have both a subjective and an objective expectation of privacy in the person or place to be searched. Even then, the governmental body may still intrude upon an individual's privacy, including searches and seizures, if government officials can convince a judge that it is more likely than not that a search of the person or place to be searched will result in the discovery of evidence of a crime or contraband, otherwise known as "probable cause". This is an essential measure of judicial oversight in the search process in the United States. Please also note that just about every State also has a similar constitutional provision, including several versions of the Fourth Amendment in State constitutions.

---

[77] Id. at p. 145

[78] Id. at 146

[79] Id.

[80] Id.

[81] Id.

[82] U.S. Const. Amend. IV.

One could further argue that the Constitutional protections referred to above are further explained and expanded by looking at the Rules of Criminal Procedure.[83] The Rules of Criminal Procedure are the Rules that are adopted by the Court System to implement the ever-present Constitutional protections.[84] A rule-by-rule analysis is beyond the scope of this article, however.[85]

3.3 Article 15 in relation to specific procedural powers

3.3.1 Expedited preservation of stored computer data (Article 16)

3.3.1.1 About article 16

The first power limited by the conditions and safeguards dictated in Article 15 is set forth in Article 16 – "[e]xpedited preservation of stored computer data."[86] The essence of this provision is to mandate that each Party provide a particular type of mechanism to enable "competent authorities" to require "preservation of specified computer data, including traffic data".[87] The particularities of this power is scattered among the first three subsections of this provision. The fourth subsection merely indicates that the powers contained within this provision are subject to Articles 14 and 15.

There are a few points of interest made both within Article 16 and which are further explained in the commentary. The first is that this provision only applies to data that has already been "collected and retained by data-holders". This means that any requirements hereunder would not require any further efforts to collect or retain data that already has not been so collected or retained.[88] The Commentary goes on to explain that Articles 16 and 17 explicitly do not address the issue of when a data holder has not already preserved said target data.[89] Paragraph 152 of the Explanatory Report summarizes as follows: "[t]he articles, therefore, provide only for the power to require preservation of existing stored data, pending subsequent disclosure of the data pursuant to other legal powers, in relation to specific criminal investigations or proceedings."[90] In

---

[83] 18 U.S.C. §§ (1 – 6003).

[84] Id.

[85] There are numerous and varied state and Federal laws within the United States aimed at the protecting its public from governmental intrusions upon their seclusion. This is such a big topic that I have pretty much limited discussion to civil liberty protections in governmental investigation of crime. I do not cover all of the instances where the Government may otherwise be prevented from accessing personal information due to legally prevented from doing so under a privacy-related legal provision.

[86] The full text of Article 16 is as follows:

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

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

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15." COE Convention on Cybercrime, Article 16.

[87] Id. at subsection 1.

[88] See Convention on Cybercrime (CETS 185) Explanatory Report, Paragraph 149.

[89] Paragraph 151 goes on at length about the difference between data preservation and data retention.

[90] See Convention on Cybercrime (CETS 185) Explanatory Report, Paragraph 152.

subsection 2 of Article 16, the Convention specifies that such power to preserve must include a provision that such preservation shall be as for long as necessary and up to ninety days. Further, there may be an option for renewal of said order.[91] This power shall only be preservation of applicable data and did not address the acquisition thereof by law enforcement.[92] In fact, the Convention addresses the very real possibility where it may take a long time for such acquisition to take place, particularly in the international investigation scenario utilizing mutual legal assistance treaties.[93]

While Article 16 requires a method to preserve, it does not dictate a lot of the details thereof. It does not mandate that such data be "frozen" or otherwise rendered inaccessible to the end user.[94] It also does not mandate the methodology used to preserve.[95] Nor does this article mandate the type of data to be preserved, beyond its bare indication that it had to be "stored by means of a computer system.[96] Article 16 does, however, mandate that there be a provision under the domestic law of a signatory State that requires the data holder to hold confidential, for a particular period of time, that they have been required to preserve said data.[97]

3.3.1.2 A perspective on conditions and safeguards in the U.S.

The first step in any legal analysis for the protection of individual rights of United States citizens against unnecessary governmental intrusion in their lives starts with the Fourth Amendment to the United States Constitution, along with its State equivalent provisions.[98] That being said, prior to the final drafting of the Convention on Cybercrime, the United States already had a provision for the preservation of stored data addressed in Article 16.

Under 18 U.S.C. §2703(f), the Federal law of the United States provides:

> "(f) Requirement To Preserve Evidence. - (1) In general. - A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evIdence in its possession pending the issuance of a court order or other process.
>
> (2) Period of retention. - Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity."

While this is a Federal law, there is no requirement that the "governmental entity" referred to therein must be a Federal governmental entity. In fact, based upon the author's experience, local prosecutors routinely have utilized this procedure to preserve evidence that would later be acquired via court order from a state and not Federal court. It should be noted that this power is not limited to prosecutors, but rather is just any governmental entity. In addition, there is no judge or other supervisory authority that must approve these actions either at the time or in retrospect. As with any governmental action, however, should its use be deemed an infraction

---

[91] Convention on Cybercrime (CETS 185) Explanatory Report, Paragraph 156.

[92] Convention on Cybercrime (CETS 185) Explanatory Report, Paragraph 156.

[93] Convention on Cybercrime (CETS 185) Explanatory Report, Paragraph 157.

[94] Convention on Cybercrime (CETS 185) Explanatory Report, Paragraph 159.

[95] Id.

[96] Convention on Cybercrime (CETS 185), Article 16(1).

[97] Convention on Cybercrime (CETS 185) Explanatory Report, Paragraph 163.

[98] US. Const. Amend. IV. Please also recognize that the scope of this article does not allow for the discussion of the delicate differences between the Fourth Amendment to the United States Constitution and the various State Constitutional provisions.

upon the civil rights of an individual, and thereby could be redressed in a civil action against said authority.[99] However, the author is unaware of any such actions being pursued.

This provision is routinely utilized throughout the United States to preserve data and to allow effective preservation of digital evidence whilst respecting the individual liberties of United States citizens. Having personally instructed many law enforcement officers and other prosecutors on its use, it is very effective to force the data holder to preserve data in its possession until other legal process can be utilized to acquire said evidence. This procedure balances the needs of law enforcement to preserve evidence and to investigate matters that would otherwise be beyond investigation due to inadvertent destruction of evidence by data holders. It should be noted however, that this does not allow a governmental authority to utilize this method with respect to just any holder of electronically stored data. There are restrictions. This provision, as do all provisions of the Stored Communications Act (SCA), only applies to those defined as an "Electronic Communications Service" or a "Remote Computing Service".[100]

3.3.2 Expedited preservation and partial disclosure of traffic data (Article 17)

3.3.2.1 About Article 17

The second power referred to in Article 15 is contained within Article 17, entitled "[e]xpedited preservation and partial disclosure of traffic data."[101] In essence, this Article modifies Article 16 by adding the requirements that the Article 16 measures be available whether or not the data to be so preserved was transmitted by more than one service provider, as well as to allow the "expeditious disclosure" to allow the Party to ascertain the Identities of the services providers and the path that such communication had been transmitted.[102] The last subsection, like in Article 16, merely states that it is subject to the provisions of Articles 14 and 15.[103]

3.3.2.2 A perspective on conditions and safeguards in the U.S.

The United States has several different avenues for safeguards and conditions with respect to the Article 17 discussions. The overarching protection is the Fourth Amendment to the United States

---

[99] This provision provides that "[e]very person who under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, Suit in equity, or other proper proceeding for redress." 42. U.S.C. §1983.

[100] This does leave open the definition of what the Stored Communications Act refers to as a "wire … communication service". See 18 U.S.C. §2703(f)(1).

[101] The term Traffic Data is defined in Article 1 of the Convention on Cybercrime as follows: "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."

[102] The full text of Article 17 is as follows:

1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15."

[103] Convention on Cybercrime (CETS 185), Article 17.

Constitution and its state equivalents. However, there is a specific framework that must be complied with in order to get the type of information held by data holders, as discussed in Article 17. This paradigm is based primarily in the SCA when applied to Federal law enforcement authorities; but, would also reach into fifty states' individual laws if state law enforcement authorities utilize the procedures set forth in their state's equivalent to the SCA. It is also noteworthy that explaining the SCA's requirements can be quite daunting. Based upon personal experience, it can be challenging in practice and I would surmise that most of the prosecutors and law enforcement officers in the United States are not fully familiar with its intricacies. That being said, while Article 17 only deals with a portion of evidence that can be obtained under the SCA, it is important to explain its requirements as a whole because once the reader becomes familiar with how it operates, the reader may then be in a better position to understand the safeguards and conditions with respect to Article 17, in particular.

The SCA provides a whole privacy protection scheme that everyone, including governmental authorities, must follow for obtaining information from what the Department of Justice labels as "network service providers".[104] The SCA has three main provisions in this respect:

- Section 2703[105] provides a mechanism that governmental officials must follow to compel disclosure from network service providers;
- Section 2702[106] regulates the voluntary relinquishment of said information to both governmental and non-governmental personnel; and
- Section 2701[107] provides criminal penalties for bypassing the procedures set forth in the previous two sections.

The drafters of the SCA provided different levels of protections to different sorts of information because they thought certain types of information deserved more protection than others. Governmental authorities must apply these levels and classifications to determine what they must do to obtain or compel the provision of this information.[108] According to the Computer Crime and Intellectual Property Section of the United States Department of Justice (CCIPS), governmental authorities should follow a three step procedure:

1. Classify the network service provider (are they an "electronic service provider" and/or a "remote computing service"?);
2. Classify the data sought; and
3. Determine if the governmental authority is going to seek to compel disclosure[109], or rather just to accept voluntary disclosure by the provider.[110]

As mentioned previously, the explanation of each of these steps is detailed and would take several pages to explain. A chart put together by CCIPS[111] summarizes this:

---

[104] Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 115 (2009). This is not from the statute itself; but, rather a different term altogether.

[105] See 18 U.S.C. § 2703.

[106] See 18 U.S.C. § 2702.

[107] See 18 U.S.C. § 2701.

[108] Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 116 (2009).

[109] If they are going to compel disclosure, then they have to determine the appropriate tool for obtaining such information (i.e. a search warrant, a 2703(d) order, or a subpoena).

[110] Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 116 (2009).

[111] Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, (2009).

	Voluntary Disclosure Permitted	**Voluntary Disclosure Permitted**	**Compelling Disclosure**	**Compelling Disclosure**
	Public Provider	**Non-public Provider**	**Public Provider**	**Public Provider**
Basic subscriber, session, and billing information	No, unless 2702(c) exception applies 2702(a)(3)	Yes 2702(a)(3)	Subpoena; 2703(d) order; or search warrant 2703(c)(2)	Subpoena; 2703(d) order; or search warrant 2703(c)(2)
Other transactional and account records	No, unless 2702(c) exception applies 2702(a)(3)	Yes 2702(a)(3)	2703(d) order or search warrant 2703(c)(1)	2703(d) order or search warrant 2703(c)(1)
Retrieved communications and the content of other stored files	No, unless 2702(b) exception applies 2702(a)(2)	Yes 2702(a)(2)	Subpoena with notice; 2703(d) order with notice; or search warrant 2703(b)	Subpoena; SCA does not apply 2711(2)
Unretrieved communications, including email and voice mail (in electronic storage more than 180 days)	No, unless 2702(b) exception applies 2702(a)(1)	Yes 2702(a)(1)	Subpoena with notice; 2703(d) order with notice; or search warrant 2703(a), (b)	Subpoena with notice; 2703(d) order with notice; or search warrant 2703(a), (b)
Unretrieved communications, including email and voice mail (in electronic storage 180 days or less)	No, unless 2702(b) exception applies 2702(a)(1)	Yes 2702(a)(1)	Search warrant 2703(a)	Search warrant 2703(a)

As you can see from the Chart, the SCA does not apply to all communications.[112] Indeed, if an entity is neither an electronic communication service, nor a remote computing service, the SCA does not apply at all. In those cases, the civil liberties of the Public are protected by requiring law enforcement authorities to obtain either a subpoena or a search warrant to compel the disclosure of the needed information. Those tools are available to law enforcement at the Federal, state and local levels.

[112] There are some differences in how the SCA is interpreted in different Court systems in the United States. Indeed, most, if not all states, have their own version of the SCA which may or may not match the SCA word for word. Thus, there may be substantial differences in how governmental authorities obtain these types of records, depending upon where they are within the United States.

3.3.3 Production Order (article 18)

3.3.3.1 About Article 18

The third requirement under the procedural law section of the Convention on Cybercrime is contained within Article 18 and is titled "Production Order".[113] Said requirement mandates the Party adopt measures to empower its authorities to order two different things[114]: 1. Specified stored data from a "person in its territory"; and 2. Subscriber information from a "service provider offering its services" in that territory. Paragraph 3 of Article 18 then goes on to define subscriber information as follows:

> "any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
> a the type of communication service used, the technical provisions taken thereto and the period of service;
> b the subscriber's Identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
> c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement."

The Explanatory comments to the convention provide additional insights that are especially noteworthy. It is clear that the drafters wanted the Parties to have the option of pursuing a court order of certain information rather than utilize what they characterized as search and seizure methods. As they put it:

> "A 'production order' provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability."[115]

---

[113] Convention on Cybercrime (CETS 185), Article 18.

[114] The full language of Article 18 is as follows:

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement."

[115] Convention on Cybercrime (CETS 185) Explanatory Report, Paragraph 171.

This is an important distinction when discussing conditions and safeguards, as the Drafters clearly had contemplated additional measures with regard to privilege and confidentiality. The Explanatory Comments explain that Parties "may exclude privileged data or information."[116] The Drafters thought that a Party "may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers."[117] The Drafters also understood that these types of orders could be used as a precursor to further efforts to obtain evidence by means of search and seizure methodologies. Thus, while there is no reference in Article 18 itself to require or merely encourage a provision mandating the person receiving such an order keep its existence confidential, paragraph 175 clearly indicates that the Drafters supported the Idea of such a provision in a Parties' domestic legislation.[118]

3.3.3.2 A perspective on conditions and safeguards in the U.S.

Being familiar with the United States laws and regulation with regard to disclosure of the information contemplated by Article 18, it is evident that the United States laws provide various conditions and safeguards for the situations delineated in Article 18. They are not simple to describe, however.

At the Federal level, one may again look to the protections set forth in the SCA.[119] As you may recall, the SCA includes provisions for governmental authorities to obtain the types of information contemplated under Article 18. The SCA protects the liberties of United States citizens by providing a paradigm for obtaining types of digital evidence from persons, depending upon the type of information requested and whether that person functions as "electronic communications service" (ECS) and or a "remote computing service" (RCS), as set forth under the Article 17 discussion above.[120] As these were discussed at length with regard to service providers in the previous section, there is no need to revisit them at this time.

The United States law is less clear on the mandates of Article 18(1)(a), however. The SCA and its state equivalents only apply to entities it characterizes as an ECS or RCS with respect to the information being requested. With respect "persons" not characterized as an ECS or RCS, the answer of the United States perspective is less clear. Clearly, competent authorities can use a search warrant, as can be discussed in the next section. While that is a court order, in and of itself, the Drafters, I believe, were not referring that sort of power. Competent authorities could use a subpoena to obtain certain types of information; however, the law is not clear whether any competent authority could merely use a subpoena to obtain information from an individual person that does not qualify as an RCS or ECS.[121] This is so because the SCA governs not only to provide a method to force disclosure; but it is also mandates when and to whom the covered information may be voluntarily disclosed.

In similar matters in civil cases, parties have attempted to use subpoenas to obtain electronic records and have been prohibited from doing so. One example of the confusion, as well as the protections present to protect civil liberties can be seen by looking at how the SCA has been

---

[116] Convention on Cybercrime (CETS 185) Explanatory Report, Paragraph 174.

[117] Convention on Cybercrime (CCETS 185) Explanatory Report, Paragraph 174.

[118] Convention on Cybercrime (CCETS 185) Explanatory Report, Paragraph 175.

[119] 18 U.S.C. §2701 et seq.

[120] Id.

[121] This is a point of disagreement. First, one must know whether we are discussing an purely Federal prosecution or one that includes state authorities. The state authorities likely could use a state-based statute that is very similar to the SCA. Second, there is not much law on whether law enforcement could use a regular subpoena and not one issued under the SCA.

applied in the social networking context.[122] In *Crispin v. Audigier, Inc.*[123], for example, the Defendants subpoenaed communications related to the Plaintiff from MySpace, FaceBook and a web host. Crispin filed motions to quash the subpoenas. The Court ruled that the data requested should be afforded the protection of the SCA, as all three providers were acting as ECSs and RCSs for those communications.[124] Consequently, the Court quashed the subpoenas.[125]

3.3.4 Search and seizure of stored computer data (Article 19)

3.3.4.1 About Article 19

In order to examine the conditions and safeguards contemplated by the requirements agreed to in Article 19[126], one must examine Article 19 itself. This article is titled "[s]earch and seizure of stored computer data" and is comprised of five paragraphs. At its essence, this article attempts to input the requirement that Parties have some legal mechanism to obtain, search and retain computer data in whatever form it may be found.[127] The Article itself is broken down into five paragraphs.[128] The first paragraph provides for the general power to search for computer data stored in any medium within its territory. The second paragraph provides that each Party shall adopt a measure that allows its authorities to "expeditiously extend the search or similar accessing to" any other system where it has grounds to believe that the data sought is not just in the system, if at all, they have searched or seized, but rather in some additional system.[129] The third paragraph provides for seizure, retention, maintenance and rendering inaccessible and/or removal

---

[122] For an interesting discussion of this case, please see E-Discovery of Social Media Networks Under the Stored Communications Act, Rippey, Perryman and Robertson, EDDE Journal, ABA Section of Science & Technology Law, Vol. 2, Issue 2, p. 30. (Spring 2011).

[123] 717 F.Supp. 2d 965 (C.D. Cal. 2010).

[124] Id.

[125] Id.

[126] The full text of Article 19 of the Convention on Cybercrime is provided below:

"1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15."

[127] Convention on Cybercrime (CETS 185), Article 19.

[128] Id.

[129] Convention on Cybercrime (CETS 185), Article 19(2).

of the data referred to in the first two paragraphs.[130] It directs each Party to adopt a measure that allow its authorities "to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information to enable undertaking of the measures referred to in paragraphs 1 and 2."[131] The last paragraph again merely indicates that the powers and procedures called for are also subject to the limitations of Articles 14 and 15.[132]

The Explanatory Comments provide further explanation of several topics contained in Article 19 that may be subject to disagreement or broad differences in interpretation. First, it makes clear that the main purpose of Article 19 "is to establish an equivalent power" to search for and seize intangible data just like the Parties' domestic law would allow for same with regard to tangible property.[133] However, Article 19 does address some particularities. For instance, the comments make clear that whether data searched for and seized would be considered stored or in-transit (thereby implicating other powers to obtain) is up the individual country's domestic law.[134] Likewise, the Comments make clear that this provision is not addressing transborder searches.[135] The Comments go on to explain many interpretations of Article 19, but one that is significant is contained in paragraph 200. Therein, the Drafters stated that it may be necessary for a system administrator to assist the search and or seizure, and that adding a provision to mandate same helps not only the competent authorities, but also the person or business being searched so as to allow that person or business to get on with their work as soon as possible.[136]

3.3.4.2 A perspective on conditions and Safeguards in the U.S.

It is a basic tenant of American law that its citizens are protected from unnecessary governmental intrusion upon their affairs by the Fourth Amendment to the United States Constitution, as well as its state equivalents.[137] This was discussed at length above.

Case law within the United States established that the protections of the Fourth Amendment applied not only to searches of tangible property, but also of the data contained within that property.[138] The search warrant methodology is routinely used in Federal and state criminal investigations across America and it is unlikely to ever change. It is one of the basic and most effective protections that American citizens have against infringement of their liberties by any branch of the government located within the territory of the United States.

Whether the Government uses a search warrant in an investigation, however, does not limit them from using the other tools in their investigation to obtain evidence. The only one applicable in this portion of this paper would be seizure by consent. If a party with disposition and control over a piece of digital evidence voluntarily provides that to the law enforcement authorities, they may take possession, copy and conduct appropriate search and analysis as if such information was obtained through a valid search warrant. Even though consent may be later withdrawn,[139] the revocation does not operate to vitiate the information obtained by the law enforcement authorities

---

[130] Convention on Cybercrime (CETS 185), Article 19(3).

[131] Convention on Cybercrime (CETS 185), Article 19(4).

[132] Convention on Cybercrime (CETS 185), Article 19(5).

[133] Convention on Cybercrime (CETS 185) Explanatory Comments, paragraph 184.

[134] Convention on Cybercrime (CETS 185) Explanatory Comments, paragraph 190.

[135] Convention on Cybercrime (CETS 185) Explanatory Comments, paragraph 195.

[136] Convention on Cybercrime (CETS 185) Explanatory Comments, paragraph 200.

[137] U.S. Const. Amend. IV

[138] See e.g. United States v. Comprehensive Drug Testing, 621 F.3d 1162 (9th Cir. 2010).

[139] See United States v. Jackson, 598 F.3d 340 (7th Cir. 2010) (stating that consent can be withdrawn at any time).

whilst the consent was still valid and in effect.[140] This means that the law enforcement authorities could immediately search evidence given to them and use the evidence observed as support for a subsequent search warrant should the original consent be withdrawn.

While the search warrant requirement in the United States goes a long way to protecting the civil liberties of people and businesses within its borders, there are also many exceptions to the methodology. Some of those exceptions include: plain view, automobile exception, exigent circumstances, administrative exceptions, consent, open fields, search incident, border searches, as well as others.[141] In each of those exceptions, however, it is very likely that if a person were to be arrested and charged as a result, that person would challenge the constitutionality of said search. They may do so in any criminal proceeding in the United States by filing Motion to Supress the evidence obtained in the questionable manner. Should the Court so find that the evidence was not properly obtained pursuant to the exception the warrant requirement, all said evidence, as well evidence that was later obtained as a result of having the evidence originally obtained in the objectionable manner, would be excluded from being entered into evidence in any criminal prosecution within the United States against the person whose rights were so violated. This is called the Exclusionary Rule[142] and is one the most utilized civil liberties protection within the legal system in the United States and is basic tenant of the protection of our citizens against abuse of power by our government.

One of the more controversial uses of the exceptions with regard to intangible evidence in the recent past has been the border search exception. Under said exception, law enforcement authorities may search for and seize anything belonging to an individual entering into the United States of America.[143] According to recently released statistics, about 6,500 individuals have had their laptops searched since 2008.[144] The authorities have in the past seized and searched laptop computers of individuals entering the United States without having any articulable suspicion of wrongdoing, let alone probable cause. This has raised the ire of many individuals due to the popular opinion that said exercise of authority is an abuse of power. As is normally the case in America, if the public greatly dislikes something, believing it to be an abuse of power, their elected governmental officials likely would investigate said actions. The public's distaste for such policies in America gave rise to such an investigation, which lead to a very public change of policy by the Executive Branch of the United States government. One could argue, therefore, that public outcry, followed by pressure from their elected officials, certainly could lead to an unofficial way of protecting civil liberties in the United States. This is a great example, given that the practices employed in searches conducted by some border agents were not technically illegal. However, because people had such concern over their privacy, the Government actually changed its policies.

---

[140] See Lee v. City of Chicago, 330 F.3d 456 (7th Cir. 2003)(stating that while consent can be withdrawn at any time information obtained whilst consent was in effect can still be used if that search revealed probable cause).

[141] See Kansas v. Ibarra 147 P.3d 842 (Kan. 2006)(basically explaining search warrant requirement exceptions).

[142] It is noteworthy, however, that the Exclusionary Rule does not dictate that the evidence so obtained be destroyed. In fact, this evidence could be obtained for use in a civil proceeding.

[143] United States v. Arnold, 2008 WL 1776525 at 4 (9th Cir. 2008)

[144] See Suspicionless Border Searches of Electronic Devices: Legal and Privacy Concerns with the Department of Homeland Security's Policy, Constitution Project (May 19, 2011). Available May 20, 2011 at: http://www.constitutionproject.org/pdf/Border_Search_of_Electronic_Devices_0518_2011.pdf.

3.3.5 Real time collection of traffic data (Article 20) and interception of content data (Article 21)

3.3.5.1 About Articles 20 and 21

The requirements of Article 20 and 21 are discussed together in this section because they both deal with the collection of data in real-time.[145] As opposed to the powers called for in the previously discussed articles, Articles 20 and 21 deal with legal authority to collect and or intercept the future transmission of data and not merely preservation or collection of data already in someone's possession.[146] Article 20 deals only with real-time collection of "traffic data"[147], whereas Article 21 covers interception of the actual content of those communications[148]. Each section is extremely similar, only really differing on the above points. Each requires the Parties to adopt measures to empower competent authorities to either collect such targeted data itself, or have the option of compelling a service provider to collect such data on behalf of the government, or at least to cooperate and assist those authorities in the collection and/or recording of same.[149] The provisions both go on to state that if such powers cannot be had pursuant to the domestic law

---

[145] Convention on Cybercrime (ETS 185) Articles 20 & 21. Please also note that the Convention itself groups them together under Title 5 "Real-time collection of computer data".

[146] Convention on Cybercrime (ETS 185) Explanatory Comments, paragraph 208.

[147] Convention on Cybercrime (ETS 185) Articles 20. The full text of Article 21 is as follows:

"1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15."

[148] Convention on Cybercrime (ETS 185) Articles 21. The full text of Article 21 is as follows:

"1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15."

[149] Convention on Cybercrime (ETS 185) Articles 20 & 21.

then in place, it is sufficient to enact means that ensure that said recording can take place. Each Article also has a specific provision that requires the Party to adopt measures that compel a service provider to keep confidential "the fact of the execution of any power provided" under either Article, including "any information relating to" the execution of those powers.[150] [151]

The Explanatory Comments to these Articles further refine the intent of the Drafters. In paragraph 206, the Comments make clear that the Articles are referring to both communications over regular computer networks and telecommunications over those same networks.[152] The exact types of data are further delineated, as follows:

> "'Traffic data' is defined in Article 1 d to mean any computer data relating to a communication made by means of a computer system, which is generated by the computer system and which formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size and duration or the type of service. 'Content data' is not defined in the Convention but refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)."[153]

Recognizing that different Parties' domestic legal systems may treat the actions called for in these Articles quite differently, the Comments also specify that scope of these provisions shall be left open the Parties.

Due to the obvious invasive nature of the powers to be granted to law enforcement authorities pursuant to Articles 20 and 21, the Comments make clear that "stringent safeguards are required to ensure an appropriate balance between the interests of justice and the fundamental rights of the individual."[154] The comments go on to specify:

> "In the area of interception, the present Convention itself does not set out specific safeguards other than limiting authorisation of interception of content data to investigations into serious criminal offences as defined in domestic law. Nevertheless, the following important conditions and safeguards in this area, applied in domestic laws, are: judicial or other independent supervision; specificity as to the communications or persons to be intercepted; necessity, subsidiarity and proportionality (e.g. legal predicates justifying the taking of the measure; other less intrusive measures not effective); limitation on the duration of interception; right of redress. Many of these safeguards reflect the European Convention on Human Rights and its subsequent case-law … Some of these safeguards are applicable also to the collection of traffic data in real-time."[155]

The Comments finally states that the communications will be considered as being within the Party's territory if either one of the parties to the communication are located within that territory, or if the communication is routed through that territory.[156]

---

[150] Convention on Cybercrime (ETS 185) Articles 20(3) & 21(3).

[151] Each section does also have a paragraph 4 which again merely states that requirements of the respective articles are explicitly subject to Articles 14 and 15.

[152] Convention on Cybercrime (ETS 185) Explanatory Comments, paragraph 206.

[153] Convention on Cybercrime (ETS 185) Explanatory Comments, paragraph 209.

[154] Convention on Cybercrime (ETS 185) Explanatory Comments, paragraph 206.

[155] Convention on Cybercrime (ETS 185) Explanatory Comments, paragraph 206.

[156] Paragraph 227 also discusses an interesting issue. Therein, the comments make mention that a stronger privacy concern could exist where data can be derived about the source or destination of a communication, such as web sites visited. Convention on Cybercrime (ETS 185) Explanatory Comments, paragraph 227.

3.3.5.2 A perspective on conditions and Safeguards in the U.S.

The collection and interception of data in real-time in the United States primarily is governed by two statutes: the Pen Register and Trap and Trace statute (the "Pen/Trap" statute")[157] and the Wiretap Act.[158] The former controls the collection of "addressing and other non-content information for wire and electronic communications",[159] while the latter regulates "collection of actual content of wire and electronic communications."[160] They are very different mechanisms in practice.[161]

3.3.5.2.1 Pen/Trap Statute

In order to take advantage of the investigative tools in the Pen/Trap statute, an attorney acting on behalf of the government must apply for a court order. To obtain this order, the applicant must "Identify themselves, Identify the law enforcement agency conducting the investigation, and then certify their belief that the information likely to be obtained is relevant to an ongoing criminal investigation be conducted by the agency."[162] As long as those elements are present and the Court has jurisdiction over the offense being investigated, the Court must issue the order.[163] There really is no independent investigation by the Court into the truth of the statements made in the application, however. Thus, judicial oversight is a constant safeguard in even the collection of addressing information in real-time. In order to get such an order and to install a pen register or trap and trace device, the applicant must merely show that "the information likely to be obtained is relevant to an ongoing investigation."[164]

Generally, "a pen register records outgoing addressing information (such as a number dialed from a monitored telephone), and a trap and trace device records incoming addressing information (such as caller ID information)."[165] However, the Pen/Trap statute also applies to other technologies and will include those with regard to networked computer communications.[166] In particular, because internet communication "headers" contain indications of where that communication was going to and where it is coming from, both pen registers and trap and devices are simply referred to pen/trap devices.[167]

While there is not a large judicial inquiry into getting one of these orders, the government is very restricted in what kinds of technology it can use in order to assure that no content information is collected in the process. Generally, the statute merely requires that government must use "technology reasonably available to it" to avoid collecting the content of communications.[168] In

---

[157] 18 U.S.C. §§ 3121-3127.

[158] 18 U.S.C. §§ 2510-2522.

[159] Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 151 (2009).

[160] Id.

[161] See Search and Seizure Manual, infra, citing United States Telecom Ass'n v. FCC, 227 F. 3d 450, 453-454 (D.C. Cir. 2000), among others.

[162] Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 154 (2009). See also 18 U.S.C. § 312(b)(1) – (2).

[163] Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 155 (2009).

164 18 U.S.C. § 3122(b)(2).

[165] Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 153 (2009).

[166] Id., citing, In re Application of the United States, 416 F. Supp. 2d 13, 16 (D.D.C. 2006).

[167] Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 154 (2009).

[168] See Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 155 (2009) & 18 U.S.C. § 3121(c).

practice, however, courts have largely prohibited the use of pen/trap devices that collect any kind of content whatsoever.[169] Likewise, there are substantial criminal penalties, including possible imprisonment and fines, should the pen/trap statute be violated.[170]

3.3.5.3 The Wiretap Act

Originally enacted in 1968 as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Wiretap Act has long permitted the interception of the contents of communications within the United States. However, judicial oversight is intense as the protection of the civil liberties of the public is a constant and primary concern.

The Wiretap Act prohibits the interception of any wire, oral or electronic communication between the parties to that communication unless one of several statutory exceptions apply.[171] This is a blanket prohibition, no matter where in the United States the communication is being made. It is also noteworthy that most, if not all, States have similar prohibitions within their State criminal codes, as well.[172] Because of this general prohibition, investigators generally must pursue exceptions thereto, seven of which are applicable to computer investigations, in general.[173]

One of the main exceptions to the general prohibition of collection of such data is when the collection is pursuant to a court order, as set forth under 18 U.S.C. § 2518, or Wiretap Order. Generally, only high level officials of the Department of Justice may even apply for such an order. In practice, very, very few people actually have this authority at the Federal level, with even fewer state law and local law enforcement officials.

The Search and Seizure Manual succinctly sets forth the extensive requirements for obtaining such an order:

> "Title III imposes several formidable requirements that must be satisfied before investigators can obtain a Title III order. *See* 18 U.S.C. §§ 2516-2518. Most importantly, the application for the order must show probable cause to believe that the interception will reveal evidence of a predicate felony offense listed in § 2516. *See* § 2518(3)(a)-(b). For federal agents, the predicate felony offense must be one of the crimes specifically enumerated in § 2516(1)(a)-(s) to intercept wire communications, or any federal felony to intercept electronic communications. *See* 18 U.S.C. § 2516(3). The predicate crimes for state investigations are listed in 18 U.S.C. § 2516(2). The application for a Title III order also (1) must show that normal investigative procedures have been tried and failed, or reasonably appear to be unlikely to succeed or to be too dangerous, *see* § 2518(1)(c); and (2) must show that the surveillance will be conducted in a way that minimizes the interception of communications that do not provide evidence of a crime. *See* § 2518(5)."[174]

---

[169] Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 156 (2009).

[170] See 18 U.S.C. § 3121(d). See also Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, pp. 157-158 (2009).

[171] 18 U.S.C. §§ 2510(4), 2511(1). See also Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, pp. 161 (2009.

[172] Please see the Search and Seizure for an excellent discussion of the Wiretap, or "Title III" as they refer to it. I depended upon that document extensively in the preparation of this paper. I also referred to often when I was a prosecutor.

[173] See Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 167 (2009)

[174] See Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 167 (2009)

Should law enforcement authorities knowingly or unwittingly violate the Wiretap Act, there can be severe sanctions including criminal penalties[175], civil liability[176] and possibly suppression of evidence.[177] [178] The protection of the privacy of the public at large in the United States is sometimes a point of contention. However, it is strongly believed that there are significant and constant protections in place to protect against any sort of improper interception of the content of communications by any governmental entity in the United States.[179]

3.4 Effects on international cooperation

The conditions and safeguards presently existing in the United States have many ramifications to foreign nationals possessing data within the United States. While the scope of this paper does not allow discussion of too many specifics, it is clear that the conditions and safeguards in place largely will apply to protect the privacy of those foreign nationals, as well as United States citizens. The recent case involving Wikileaks provides a great example.

In a recent United States District Court decision for the Eastern District of Virginia, the Court held that personally identifiable information is discoverable in a case where foreign nationals made use of social media software based in the United States of America.[180] In *In Re: §2703(d) Order,* Twitter users[181] associated with account names of interest to the ongoing investigation into the Wikileaks scandal petitioned the government to vacate an order of a lower court to turn over information associated with their respective accounts. The discovery order (Twitter Order) required Twitter, Inc., a social network service provider, to turn over to the United States subscriber information concerning accounts associated with the Wikileaks investigation pursuant to the Stored Communications Act.[182]

The Twitter Order required Twitter, Inc. to present to the court: subscriber names, user names, screen names, or other Identities; mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information; connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or Identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number) and billing records.

After review of the legal issues presented in the petitioners' arguments[183] the court ultimately upheld the validity of the Twitter Order. In its official opinion, the Court found the petitioners' assertions that the Twitter Order violated their rights under the First Amendment and Fourth Amendment largely unpersuasive. In both instances, the court cited the fact that the petitioners'

[175] See 18 U.S.C. § 2511(4).

[176] See 18 U.S.C. § 2520.

[177] See 18 U.S.C. § 2518(10)(a).

[178] See Search and Seizure Manual, Computer Crime & Intellectual Property Section, United States Department of Justice, p. 183 (2009).

[179] Please note that this article does not discuss protections to civil liberties under the laws pertaining to national security as it is beyond the scope of this article.

[180] In Re: §2703(d) Order, 10GJ3793 (E.D. Va. 2011).

[181] Jacob Appelbaum (Twitter name "ioerror"), a United States citizen and resident, Rop Gonggrijp (Twitter name "rop_g") a Dutch citizen, and Birgitta Jonsdottir (Twitter name "birgittaj") an Icelandic citizen and resident.

[182] 18 U.S.C. §§ 2701-2711 (2000 & Supp. 2009).

[183] (1) whether petitioners have standing under the Stored Communications Act ("SCA") to bring a motion to vacate, (2) whether the Twitter Order was properly issued under 18 U.S.C. §2703, (3) whether the Twitter Order violates petitioners' First Amendment rights, (3) whether the Twitter Order violates petitioners' Fourth Amendment rights, and (4) whether the Twitter Order should be vacated as to Ms. Jonsdottir for reasons of international comity.

willingly presented their Twitter messages to the public and provided personally identifiable information to Twitter, Inc. as a primary reason to invalidate their arguments under First and Fourteenth Amendments.

Of greater consequence, the court also held that the petitioners' challenge under the Stored Communications Act to be prima facially invalid as well. Pursuant to §2704(b)(1)(A) of the Stored Communications Act, a customer may challenge a §2703(d) order only upon an affidavit "stating that the applicant is a customer or subscriber to the service from which the *contents* of electronic communications maintained for him have been sought.".[184] Consequentially, targets of court orders for non-content or records information may not bring a challenge under 18 U.S.C. §2704.

The Stored Communications Act provides greater protection to the "contents of electronic communications" than to their "records". Under the Act, the definition of "contents" is "any information concerning the substance, purport, or meaning of that communication."[185] Targets of content disclosures are authorized to bring a customer challenge under §2704. Conversely, §2703(c)(1) describes "records" as "a record or other information pertaining to a subscriber to or customer of such service (not the contents of communication)." As the Twitter Order did not demand the contents of any communication, only that of non-content account information, the court ultimately held that the petitioners were unable to challenge the order under such grounds.

While one could argue that there are circumstances where foreign nationals may not be provided arguably the same protection as citizens of the United States, the safeguards and protections presently in place will serve to protect foreign nationals.[186] Even if the Petitioners did not get the relief they were seeking, at least there was a mechanism in place to seek the remedies they desired. No countries legal systems are perfect, however. And there has been significant criticism of the SCA, as detailed below. People will always disagree on the balance between privacy and protection of the public.

3.5 The future of cyberspace privacy protection?

There has been much criticism of the manner in which the Federal and state governments have gone about protecting civil liberties in the course of their attempts to keep cyberspace safe. Indeed, no matter what law you examine, you most likely will find someone ready to criticize it. In its most recent incarnation, there has been a movement to change the Federal and state laws with regard to accessing stored electronic data.

As set forth above, in order for governmental entities to obtain access to stored electronic records or to access to data in transit, they must comply with the Federal Wiretap Act[187] and/or the Stored Electronic Records Act[188]. This is, of course, in addition to their state equivalents. Both sides to the ongoing privacy debate in the United States generally want revisions to these laws. In fact, the New York Times, earlier this year published an article showing how technology has outstripped this law in particular.[189] This concept that United States law is in need of substantial review is further buttressed by the public outcry when it was revealed that Apple and Android location-

[184] 18 U.S.C. §§ 2701-2711 (2000 & Supp. 2009.

[185] 18 U.S.C. §2711(1); 18 U.S.C. §2510(8)(2002).

[186] It appears that the location of the data may play a role on whether certain protections will apply to foreign nationals. Compare Suzlon Energy Ltd. V. Microsoft Corp., 9th Cir., No. 10-35793 (holding that ECPA protections applied to foreign nationals, where data was held in the United States) to Zheng v. Yahoo! Inc., No. 08-1068 (9th Cir. Dec. 2, 2009)(declining to apply the ECPA to interceptions of email that occurred outside of the United States).

[187] 18 U.S.C. §2510 et seq.

[188] 18 U.S.C. §2701 et seq.

[189] Helft, Miguel and Claire Cain Miller, "News Analysis: 1986 Privacy Law Is Outrun by the Web", The New York Times, January 9, 2011.

aware devices were keeping and transmitting user data and that the users had very little, if any, control over same once they gave their initial permissions to use the devices.[190] This area of the law was highlighted in recent Congressional hearings before the newly created Senate Subcommittee on Privacy, Technology and the Law, wherein Justin Brookman testified that "once an app has access to a user's data, there are usually no rules governing its disclosure and no controls available to consumers to regain control of it."[191]

One of the most interesting developments has been a new multidimensional group calling for significant reform of the ECPA. They call themselves "Digital Due Process" and are calling for reform of the ECPA because of many reasons, including:

- "Conflicting standards and illogical distinctions: ECPA sets rules for governmental access to email and stored documents that are not consistent. A single email is subject to multiple different legal standards in its lifecycle, from the moment it is being typed to the moment it is opened by the recipient to the time it is stored with the email service provider. To take another example, a document stored on a desktop computer is protected by the warrant requirement of the Fourth Amendment, but the ECPA says that the same document stored with a service provider may not be subject to the warrant requirement.
- Unclear standards: ECPA does not clearly state the standard for governmental access to location information.
- Judicial criticism: The courts have repeatedly criticized ECPA for being confusing and difficult to apply. The Ninth Circuit in 2002 said that Internet surveillance was "a confusing and uncertain area of the law." In the past 5 years, no fewer than 30 federal opinions have been published on government access to cell phone location information, reaching a variety of conclusions.
- Constitutional uncertainty: The courts are equally conflicted about the application of the Fourth Amendment to new services and information. A district court in Oregon recently opined that email is not covered by the constitutional protections, while the Ninth Circuit has held precisely the opposite. Last year, a panel of the Sixth Circuit first ruled that email was protected by the Constitution and then a larger panel of the court vacated the opinion."[192]

These calls for reform have not gone unheard. In 2009, President Barrack Obama put forth document entitled his "Cyberspace Policy Review."[193] Therein, he stated that the "cyber threat is one of the most serious economic and national security challenges we face as a nation."[194] Almost two years later, the Obama administration, in response to requests from Congress, issued a Cybersecurity Legislative Proposal for Congress to consider.[195] Among the reforms proposed, is a "New Framework to Protect Individual's Privacy and Civil Liberties."[196] While this does not solely address such intrusions related just in relation to criminal procedures, it sets forth proposals to several laws, including the following provisions:

---

[190] See Google, Apple Glean Computer Locations, B1, Wall Street Journal, Wednesday, April 27, 2011.

[191] See summary of testimony put forward by Mr. Brookman's employer, the Center for Democracy and Technology, at www.cdt.org/print/18460.

[192] http://www.digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163

[193] See "Cyberspace Policy Review", available at: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[194] Id.

[195] See "Cybersecurity Legislative Proposal", available at: http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf.

[196] Id.

> "I— t requires DHS[197] to implement its cybersecurity program in accordance with privacy and civil liberties procedures. These must be developed in consultation with privacy and civil liberties experts and approved by the Attorney General.
>
> All federal agencies who would obtain information under this proposal will follow privacy and civil liberties procedures, again developed in consultation with privacy and civil liberties experts and with the approval of the Attorney General.
>
> All monitoring, collection, use, retention, and sharing of information are limited to protecting against cybersecurity threats. Information may be used or disclosed for criminal law enforcement, but the Attorney General must first review and approve each such usage.
>
> When a private-sector business, state, or local government wants to share information with DHS, it must first make reasonable efforts to remove Identifying information unrelated to cybersecurity threats.
>
> The proposal also mandates the development of layered oversight programs and congressional reporting.
>
> Immunity for the private-sector business, state, or local government is conditioned on its compliance with the requirements of the proposal."[198]

One may plainly review the exact proposed legal changes that purport to make up this new framework by reviewing the section-by-section analysis that the Federal government released at the same time as the proposal itself.[199] While this is just a legislative proposal, many of the exact legal modifications set forth therein have a realistic chance of becoming law in the coming months. Even if that does not come to fruition, however, the Proposal itself sheds significant light on the present administration's priorities in this arena.

In conclusion, the safeguards and conditions envisioned under Article 15 are both substantive and intensive. However, they are also somewhat open to interpretation due to the nature of the Convention and how it was developed and adopted. Whether or not the reader believes that the civil liberties protections under United States Federal and state laws are adequate in today's world, the United States has had some of these types of conditions and safeguards in place prior to the Convention ever being developed. Nevertheless, the United States law on these issues is constantly evolving based upon commentary of its citizens and initiatives of both domestic and foreign governments.

---

[197] This acronym stands for the United States Department of Homeland Security.

[198] See "Fact Sheet: Cybersecurity Legislative Proposal", available at: http://www.whitehouse.gov/sites/default/files/fact_sheet-administration_cybersecurity_legislative_proposal.pdf.

[199] Several of the reviews are available at the official Presidential web site here: http://www.whitehouse.gov/omb/legislative_letters.

4 Appendix:

4.1 Extracts of the Budapest Convention and explanatory report

4.1.1 Article 14: Scope of procedural provisions

4.1.1.1 Text of the Convention

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
- a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
- b other criminal offences committed by means of a computer system; and
- c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
- i is being operated for the benefit of a closed group of users, and
- ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

4.1.1.2 Explanatory report

Scope of procedural provisions (Article 14)

140. Each State Party is obligated to adopt such legislative and other measures as may be necessary, in accordance with its domestic law and legal framework, to establish the powers and procedures described in this Section for the purpose of "specific criminal investigations or proceedings."

141. Subject to two exceptions, each Party shall apply the powers and procedures established in accordance with this Section to: (i) criminal offences established in accordance with Section 1 of the Convention; (ii) other criminal offences committed by means of a computer system; and (iii) the collection of evidence in electronic form of a criminal offence. Thus, for the purpose of specific criminal investigations or proceedings, the powers and procedures referred to in this Section shall be applied to offences established in accordance with the Convention, to other criminal offences committed by means of a computer system, and to the collection of evidence in electronic form of a criminal offence. This ensures that evidence in electronic form of any criminal offence can be obtained or collected by means of the powers and procedures set out in this Section. It ensures an equivalent or parallel capability for the obtaining or collection of computer data as exists under traditional powers and procedures for non-electronic data. The Convention makes it explicit that Parties should incorporate into their laws the possibility that information contained in digital or other electronic form can be used as evidence before a court in criminal proceedings, irrespective of the nature of the criminal offence that is prosecuted.

142. There are two exceptions to this scope of application. First, Article 21 provides that the power to intercept content data shall be limited to a range of serious offences to be determined by domestic law. Many States limit the power of interception of oral communications or telecommunications to a range of serious offences, in recognition of the privacy of oral communications and telecommunications and the intrusiveness of this investigative measure. Likewise, this Convention only requires Parties to establish interception powers and procedures in relation to content data of specified computer communications in respect of a range of serious offences to be determined by domestic law.

143. Second, a Party may reserve the right to apply the measures in Article 20 (real-time collection of traffic data) only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories is not more restricted than the range of offences to which it applies the interception measures referred to in Article 21. Some States consider the collection of traffic data as being equivalent to the collection of content data in terms of privacy and intrusiveness. The right of reservation would permit these States to limit the application of the measures to collect traffic data, in real-time, to the same range of offences to which it applies the powers and procedures of real-time interception of content data. Many States, however, do not consider the interception of content data and the collection of traffic data to be equivalent in terms of privacy interests and degree of intrusiveness, as the collection of traffic data alone does not collect or disclose the content of the communication. As the real-time collection of traffic data can be very important in tracing the source or destination of computer communications (thus, assisting in identifying criminals), the Convention invites Parties that exercise the right of reservation to limit their reservation so as to enable the broadest application of the powers and procedures provided to collect, in real-time, traffic data.

144. Paragraph (b) provides a reservation for countries which, due to existing limitations in their domestic law at the time of the Convention’s adoption, cannot intercept communications on computer systems operated for the benefit of a closed group of users and which do not use public communications networks nor are they connected with other computer systems. The term "closed group of users" refers, for example, to a set of users that is limited by association to the service provider, such as the employees of a company for which the company provides the ability to communicate amongst themselves using a computer network. The term "not connected with other computer systems" means that, at the time an order under Articles 20 or 21 would be issued, the system on which communications are being transmitted does not have a physical or logical connection to another computer network. The term "does not employ public communications networks" excludes systems that use public computer networks (including the Internet), public telephone networks or other public telecommunications facilities in transmitting communications, whether or not such use is apparent to the users.

4.1.2 Article 15: Conditions and safeguards

4.1.2.1 Text of the Convention

Article 15 – Conditions and safeguards

1 Each Party shall 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 under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

4.1.2.2 Explanatory report

Conditions and safeguards (Article 15)

145. The establishment, implementation and application of the powers and procedures provided for in this Section of the Convention shall be subject to the conditions and safeguards provided for under the domestic law of each Party. Although Parties are obligated to introduce certain procedural law provisions into their domestic law, the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. These domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise. The modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure. Parties shall ensure that these conditions and safeguards provide for the adequate protection of human rights and liberties. There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments. These instruments include the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and its additional Protocols No. 1, 4, 6, 7 and 12 (ETS N°s 005 (4), 009, 046, 114, 117 and 177), in respect of European States that are Parties to them. It also includes other applicable human rights instruments in respect of States in other regions of the world (e.g. the 1969 American Convention on Human Rights and the 1981 African Charter on Human Rights and Peoples' Rights) which are Parties to these instruments, as well as the more universally ratified 1966 International Covenant on Civil and

Political Rights. In addition, there are similar protections provided under the laws of most States.

146. Another safeguard in the convention is that the powers and procedures shall "incorporate the principle of proportionality." Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures. Also, the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle.

147. Without limiting the types of conditions and safeguards that could be applicable, the Convention requires specifically that such conditions and safeguards include, as appropriate in view of the nature of the power or procedure, judicial or other independent supervision, grounds justifying the application of the power or procedure and the limitation on the scope or the duration thereof. National legislatures will have 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. As stated in Paragraph 215, Parties should clearly apply conditions and safeguards such as these with respect to interception, given its intrusiveness. At the same time, for example, such safeguards need not apply equally to preservation. Other safeguards that should be addressed under domestic law include the right against self-incrimination, and legal privileges and specificity of individuals or places which are the object of the application of the measure.

148. With respect to the matters discussed in paragraph 3, of primary importance is consideration of the "public interest", in particular the interests of "the sound administration of justice". To the extent consistent with the public interest, Parties should consider other factors, such as the impact of the power or procedure on "the rights, responsibilities and legitimate interests" of third parties, including service providers, incurred as a result of the enforcement measures, and whether appropriate means can be taken to mitigate such impact. In sum, initial consideration is given to the sound administration of justice and other public interests (e.g. public safety and public health and other interests, including the interests of victims and the respect for private life). To the extent consistent with the public interest, consideration would ordinarily also be given to such issues as minimising disruption of consumer services, protection from liability for disclosure or facilitating disclosure under this Chapter, or protection of proprietary interests.