Cross-Border Law Enforcement in the Information Society (v. 0.82)

Jan Trzaskowski
Copenhagen Business School[1]

This paper comprises some reflections on cross-border law enforcement in the Information Society. The paper deals with illegal acts carried out over a distance via the Internet by businesses without (any kind) of establishment in the enforcing state. The paper takes its start within the broad concept of sovereign nation states, but deals mainly with examples from European jurisdictions. This is a working paper containing theses that are being dealt with under the authors Ph.D. project.1

The author points out that there is a need for global standards on how to geographically divide marketing material on the Internet and that states should promote the dissemination of easy understandable and accessible information about the law. States should furthermore consider domesticating and privatising law enforcement along with applying alternative law enforcement such as technical enforcement and enforcement through the market.

1. States are Sovereign; Also to Restrict their own Sovereignty

A state can be defined as a collection of individuals politically organised through a government, which exercises sovereign powers over a fixed territory. The state can in accordance with its political system decide what is legal within its territory. Most states have for economical or political reasons limited their sovereignty through international agreements.

> The sovereignty of states also entails that states can decide what kind of information should not be available in the state and which media should be available within the state and under which conditions. Most media are regulated to some extent, whereas the Internet is only in recent years becoming subject to corresponding media specific regulation.[2]
>
> The Treaty of the European Union comprises the establishment and development of an internal market providing free movement of inter alia goods and services based on harmonisation. Also the establishment of the World Trade Organization (WTO) serves the purpose of improving international trade

1 www.legalriskmanagement.com, jan@extuto.dk.

2 Restricting access and use of the Internet may be politically difficult because as the community around often consider the Internet to be a sanctuary where government interference should be as limited as possible.

on a more global basis.[3]

In the 2000 EU E-Commerce Directive[4] regulation of the Internal Market was supplemented by the introduction of the Country of Origin principle,[5] which provides for home country control and mutual recognition of the so-called information society services, including inter alia commercial websites.[6] Even though the influenced area ('coordinated field') was not fully harmonized, the states would in return for limitations in enforcing own laws benefit from more efficient law enforcement at the source.

Other relevant types of international cooperation include 1) procedural harmonisation regarding recognition of foreign judgments and establishing a common framework for investigation, mutual assistance etc. and 2) substantive harmonisation leading to coordinated legal norms and rules on choice of law. Substantive harmonisation or coordination may be a prerequisite for procedural harmonisation.

2. The Internet is just a Medium

The Internet is the sum of connections between certain computers/servers. The Internet is nothing but a medium that can be used for exchanging information between people -admittedly an impressive medium with a huge potential. The Internet has not abolished time and place, but made it easy and cheap to communicate over distances.

The idea of a Cyberspace as a parallel virtual world may serve pedagogical purposes just as dividing a hard drive into folders, but these metaphors however provide limited help to the legal understanding of the Internet.

The Internet however also creates a new environment for doing wrongs at a distance. The magnitude and importance of these wrongs increases, as the Internet becomes more integrated in society and more critical processes are carried out on Internet-connected devices.

Most people who use the Internet have already experienced or heard of consequences of undesirable activities such as computer viruses, unsolicited e-mails (spam), hacking, fraud, scams, misleading advertising etc. States as such may also have moral or pecuniary interest to protect, such as protecting individuals from Nazi artefacts or gambling activities.

3 See www.wto.org

4 EU Directive 2000/31 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce).

5 Article 3 of the 2000 EU Directive on E-Commerce.

6 An Information Society Service is any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service. See Article 2, (a) of the 2000 EU E-Commerce Directive and article 1(2) of Directive 98/34 as amended by Directive 98/48.

3. Borders in Cyberspace: Damage is Done Where Harm Occurs

It is implied in the sovereignty of states that a state itself to a large extent can decide when a certain act should be deemed to have effect in that state. If harm is done to a state's interest including its inhabitants, the state may be likely to consider the act to be carried out in that state no matter which medium has been used.[7]

> It is generally accepted that a number of 'old' laws also apply to activities carried out on this 'new' medium. The main challenge in governing the Internet is how to enforce national legislation. Difficulties in (cross-border) law enforcement have often led to the description of the Internet as a lawless wild west.
>
> It has been argued that when material is first published on the Internet there is no control of who will access it and thus it would be unfair to claim jurisdiction in all states from where the material can be accessed. On the other hand it can be argued that a business publishing material on the Internet should be aware of the potential of doing harm in a large number of states.
>
> In the Yahoo! case a French Court ordered the American company to hinder French people's access to online auctions concerning Nazi artefacts. This decision was later in an American court rejected under reference to American rules of freedom of speech. Despite this Yahoo! decided to comply with the French ruling.[8]
>
> In a recent case a Dutch court ordered the British company Ladbrokes to block Dutch people's access to the companies bookmaking website.[9] The mentioned cases and a number of other cases from around the world[10] support the idea of geographical borders in Cyberspace that businesses can be expectation to observe these borders.

4. A Holistic Approach to Law Enforcement

Law enforcement is about putting law into effect. It is within the sovereign powers of a state to decide which sanctions to impose on businesses that infringe the law and how to proceed against offenders. It is also within the state's sovereignty to choose which parties can enforce which wrongs.

---

7 See Geist, Michael A., Is There a There? Toward Greater Certainty for Internet Jurisdiction, 16 Berkely Technology Law Journal, 2002, p. 1345. See also Lessig, Lawrence, The Zones of Cyberspace, 48 Stanford Law Review, 1996, p. 1403.

8 See Kang, Sungjin, Yahoo!'s battle in France and the USA, Legal Issues of Economic Integration, 29/2002, p. 195.

9 Court of Anhem, 27 January 2003. See Preter, Cristoph De, Online Gaming in the Netherlands: Farewell to Ladbrokes?, 10 February 2003, www.droit-technologie.org.

10 See also Mailland, Julien, Freedom of Speech, the Internet, and the Cost of Control: The French Example, 33 N.Y.U.J, Int'l. & pol. 1179 (2001).

The purpose of enforcing law is to seek obedience in order to protect the state and its individuals' physical and economical interests. The main goal is to prevent unlawful actions to occur. Since enforcement to ensure full compliance is yet to be proved possible, a secondary objective is to punish offenders and to compensate injured parties.

In most states a distinction between public (criminal and administrative law) and private law enforcement can be found. The distinction in Europe based is on whether the enforcement is carried out by the government or a private body respectively. There are similarities in – but far from a uniform perception of – which activities fall within these groups of enforcement. Some offences may be prosecuted under either of the enforcement systems.

There are different sanctions and procedural rules attached to either of the enforcement systems. Public law enforcement normally implies sanctions such as imprisonment, fines and disqualifications, whereas private law enforcement normally leads to damages (compensation) or establishment of rights or obligations concerning a contract (including unenforceability). Court orders such as injunctions and commands are normally found under both enforcement systems.

Considering the purpose of law enforcement, other measures than those carried out by the Judiciary may as well be considered as law enforcement. Law enforcement should be considered to be all sanctions supporting the purposes defined above. States should hence apply a holistic approach in their apportionment of sanctions in order to optimize their enforcement mix based on business expected reaction to various enforcement possibilities.

Since traditional cross-border law enforcement (through the Judiciary) is a cumbersome process – if possible at all – states should consider including alternative law enforcement measures in their enforcement palette. Below are described alternative law enforcement measures that take advantage of the technical nature of the Internet and the possibilities in using market forces.

5. Recognition of Foreign Judgements

Law enforcement is traditionally carried out through the Judiciary. Recognition of judgements is a prerequisite for carrying out the decision of a court. A judgement is recognised in the state in which the judgement has been rendered, but no state is by default obliged to recognise foreign judgments.

Cooperation between regional states has led to some agreements on recognition of certain foreign judgements. In Europe, the most important acts are the

2000 EU Brussels Regulation[11] and 1988 Lugano Convention.[12] These acts provide for the 'free movement' of civil judgements within EU and EFTA States respectively.[13]

These acts provide a system for jurisdiction and mutual recognition of judgements. Enforcement of a judgement can however be refused under certain procedural grounds or by invoking that enforcement will be in contravention of public order. The 1958 UN New York Convention[14] furthermore provides a more globally adopted system for recognition of arbitral awards.

6. Applying Foreign Law in the Offender's Homecourt

Cross-border law enforcement is about imposing the law of the enforcing state on an offender established abroad. An alternative to recognition of judgement is if a relevant foreign court applies the law of the enforcing state under litigation in the state of the offender. This requires however that a prosecutor can and will bring proceedings in that foreign court.

Private persons will normally have litigation capacity in foreign courts, whereas public authorities and private organisations may not be correspondingly recognised by foreign courts. The 1998 EU Injunction Directive[15] seeks within the EU to provide certain qualified bodies with litigation capacity with a view to seek injunctions in the homecourt of the offender. The directive however only deals with infringement of some specific directives and notably does not determine the applicable law.

It is not unfamiliar to most legal systems to apply foreign law, especially in civil law suits. States are however very reluctant when it comes to applying foreign criminal law – especially if there are discrepancies between foreign and national law.

The starting point of private international law is the contacts approach,[16] which provides that the law with the closest connection to the matter should be applied. Most states accept at least to some extent the contracting parties'

11 Council regulation No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters. This regulation replaces the EC Convention on Jurisdiction and Enforcement of Judgements in Civil and Commercial Matters (1968 Brussels Convention) from 27 September 1968. Changing the convention into an EU regulation brings the principles into a part of the EU legislation whereas the Brussels convention was an independent multilateral agreement. Denmark is as the only EU state not bound by the 2000 Brussels regulation and therefore the 1968 Brussels convention still applies between Denmark and either of the other EU member states.

12 The EC and EFTA Lugano Convention on Jurisdiction and the Enforcement of Judgements Civil and Commercial Matters from 16 September 1988.

13 Under the framework of jurisdiction laid down in the acts.

14 United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards, New York, 10 June 1958.

15 Directive 98/27/EC on injunctions for the protection of consumers' interests (19 May 1998).

16 US: Center of gravity doctrine.

freedom to choose the applicable law.

The main provisions for European harmonisation of choice of law in contract in Europe are found in the 1980 EU Rome Convention.[17] Besides laying down the contacts approach, the convention contains certain presumption rules for inter alia contracts on sale of goods and services, certain consumer contracts, insurance contracts and employment contracts.

The choice of law in tort cases is sought to be harmonised under the ongoing work on the EU Rome II Regulation.[18] The officially presented draft is based on the principle of lex loci delicti[19] for a number of situations. Most European states already apply the concept of lex loci delicti in various manners.

The country of origin principle in the 2000 EU E-Commerce Directive will most likely lead to limitations in the application of the lex loci delicti within the Internal Market, since applying the law of another state than the country of establishment would be in contravention of the principle of mutual recognition.[20]

7. Privatising Law Enforcement

If a law enforcing party wants to prosecute a foreign offender for an illegal act, which is not unlawful in the state of the offender, civil law enforcement will in a number of cases be more effective than public law enforcement. These circumstances speak in favour of attaching more civil sanctions to illegal acts.

In a descriptive case,[21] an Austrian based consumer organisation ('VKI'[22]) brought proceedings in Austria in order to stop business activities pursued by the German based Karl Heinz Henkel. The European Court of Justice sustained VKI's claim that the tort forum of the 1968 Brussels Convention then in force could be applied by the consumer organisation to obtain an injunction based on Austrian law in a preventive action.[23]

If a similar case was brought by an entity exercising public powers, the mutual recognition of the corresponding 2000 Brussels Regulation now in force could not be used – leaving the public authority worse off than a private body not exercising public powers. The public authority can within the limited scope of

17 Convention on the Law Applicable to Contractual Obligations, consolidated version (98/C 27/02).

18 Text available at http://europa.eu.int/comm/justice_home/news/consulting_public/rome_ii/news_hearing_rome2_en.htm in connection to written hearing of 3 May 2002.

19 The law of the place where the wrong took place or where it had effect.

20 See Mankowski, Peter, Das Herkunftlandprinzip als Internationales Privatrecht der e-commerce-rechlinie, Zeitschrift für vergleichende Rechtswissenschaft, 2001, p. 137.

21 Verein für Konsumenteninformation vs. Karl Heinz Henkel, ECJ Case C-167/00 (1 October 2002).

22 Verein für Konsumenteninformation. See www.konsument.at

23 In the Ladbroke case mentioned above, the Court of Anheim ruled that it had jurisdiction under the 2000 Brussels Regulation in the proceeding that was brought by the Dutch Lotto Company. See Preter, Cristoph De, Online Gaming in the Netherlands: Farewell to Ladbrokes?, 10 February 2003, www.droit-technologie.org.

the 1998 injunction directive seek injunction in the homecourt of the offender and even with uncertainties connected to the choice of law.

Since it is within the powers of a sovereign state to choose sanctions for offences, the state might as well utilize the system for mutual recognition of civil judgements within EU and EFTA by distributing litigation powers and rights to civil entities. States may even support private litigants to the extent the private litigation will not be characterized as exercising public powers.

Another type of privatising can be found where parties voluntarily seek to resolve disputes. In contractual disputes it can be beneficial to choose private conflict resolution since arbitral awards are recognised between more than 100 states under the 1958 New York Convention.

Private enforcement can also be found within self-regulation, for example in the case of the European Advertising Standards Alliance self-regulatory cross-border complaint system.[24]

8. Domesticating Law Enforcement

The sovereignty of states extends only to the territory of the state. A state can benefit from its sovereignty by taking measures, which can be carried out within the state. This can be done by imposing sanctions on nationals who contribute or in other ways support the illegal act. Domestic measures can also be imposed on persons who more or less voluntarily enter the state's territory.

In American law cases against two Russian hackers, Vasiliy Gorshkov and Alexey V. Ivanov, the FBI persuaded the two men to travel to the Unites States in order to participate in job interviews in a fictitious computer security company in Seattle created by the FBI.[25] During the meeting, the FBI recorded evidence against the hackers and obtained, through a demonstration by the hackers, access to search and copy evidence from the hackers' computers in Russia.

The mentioned approach led to conviction on a number of counts of conspiracy, various computer crimes and fraud. Since the two hackers conveniently enough were staying in the USA, the sentences could easily be enforced within U.S. territory. Though such undercover enforcement approaches may be effective, they are not allowed in a number of states.

Extradition may also be a possibility to prosecute a foreign offender. Extradition is normally based on a request from the enforcing state to the state in which the offender is located. Extradition is however most often applied in connection to custodial sanction and normally requires that the act is criminal under the law of both jurisdictions and that the enforcing state does not impose more severe sanctions than provided in the law of the extraditing state (dual criminality).[26]

24 www.easa-allianca.org.
25 U.S. Department of Justice, www.usdoj.gov/criminal/cybercrime.
26 See e.g. the 1957 Paris Conventions on extradition (13 December 1957) article 2.

If it is not possible to sue the primary offender in the enforcing state, the state may be able to keep the enforcement national by applying joint responsibility for contribution or other kinds of support to the offence. Depending on the offence in question, it may be effective to forbid users to participate in certain acts such as illegal gambling or by imposing sanctions on intermediaries who benefit from or support the illegal activity.

In contractual situations it may be practical to impose joint responsibility on payment intermediaries who then will be obliged to indemnify costumers in the case where the customer e.g. does not receive the ordered goods or exercises a right of withdrawal.

The 2000 EU E-Commerce Directive[27] prescribes some limitations to the possibility to apply joint responsibility on certain kinds of intermediaries. The directive however does not exclude such law enforcement.

9. Technical Law Enforcement

The Internet requires electricity and connections in order to function. A sovereign state can choose not to connect the state to the Internet. Between this extreme and full access lie a number of possible solutions for effective law enforcement. No sovereign state is obliged to allow access to material, which is deemed unlawful in that state, unless otherwise agreed between states.

The Internet provides effective means of control.[28] If a sovereign state chooses to give access to the Internet, the state has possibilities to block out access to certain material or material from certain destinations.[29] Existing blocking techniques may not be 100% effective, but like for most other laws full compliance is not necessary in order to have effective law enforcement.

Blocking requires control over providers of Internet access. Since access providers are normally established within the state where access is provided, the access provider will also be within the state's control. Technical enforcement can be put into an automated system, which will not impose unreasonable burdens on the access providers.

Blocking will have the effect that users in the state in question cannot access the illegal material and will then mitigate the effect of the activity. Blocking causes however no further punishment than the hindrance of availability and can notably not be used to compensate injured parties.[30]

---

27 Directive 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), 8 June 2000.

28 See Zittrain, Jonathan, Internet Points of control, Havard Law School Research paper No. 54, Boston College Law Review.

29 See Dornseif, Maximillian, Government mandated blocking of foreign Web content, md.hudora.de.

30 Technical enforcement can be used as means of enforcement in the case of cyberwars or hacker-attacks. Such means may not be applied by governments, but may be used by private parties in e.g. cases where the music industry wants to hamper exchange of music by implementing viruses in files shared on peer-to-peer networks.

10. Law Enforcement Through the Market

Market forces are a well-known effective regulator. Most businesses are to some extent vulnerable to unfavourable commenting, thus using the media can for some purposes be an alternative to enforcement through the Judiciary. In the wake of the Information Society the character and credibility of information and media has changed, but information can still be a powerful tool.

A party enforcing the law can take advantage of the possibility to influence the market through information. Information has the advantage that it can have an effect on foreign businesses without being dependent on recognition. To influence the market, the party enforcing the law may however need both credibility and access to a medium.

The market can be used to put pressure on businesses carrying out illegal activities by influencing the businesses' goodwill through e.g. warning potential costumers. It has however been seen that businesses have managed to turn such situations to their own advantage, which makes the consequences of unfavourable commenting less predictable.

The market can also be used positively by approving or evaluating certain businesses or activities in some form of trustmark scheme. As long as the information under the hallmark scheme has some significance in the market, business will have an incentive to comply with the scheme and thereby inter alia observe the law of the state in question.

The market forces can be applied in order to deter infringement, but can also be applied to punish businesses to the extent the business is vulnerable to such enforcement. Enforcement through unfavourable commenting by e.g. a public authority may have a greater effect than traditional law enforcement. The credibility of information may however dilute if the media is being used too intensively.

11. Legal Risk Management: A Business Perspective

Like states, businesses should also apply a holistic approach to assessing the legal risk involved with cross-border activities on the Internet. Firstly businesses should recognise the borders in cyberspace and direct their marketing material only to chosen states and adjust their marketing material in order to limit the legal risks.[31]

It does not matter for a business whether a loss derives from a fine or a decline in turnover caused by unfavourable commenting. Businesses should in their legal risk management procedures include assessment of not only consequences of traditional law enforcement, but also consequences of

31 A legal risk can be defined as potential financial loss due to infringement of a legal norm or having unenforceable claims.

alternative law enforcement such as technical enforcement and enforcement through the market.[32]

Pursuing cross-border business online will always involve legal risks and as businesses have scarce resources to limit these risk, businesses should apply the most cost-effective approaches until the decline in expected loss equals the thereto-attached costs.

The better the law enforcement possibilities are, the higher may the expected loss be and thus the compliance. The expected loss is a combination of the risk of being punished and the magnitude of the loss involved. The expected loss will be higher if the enforcement system is improved. Businesses should normally start by complying with national law since the best access to enforcement is found in the state of establishment.

The most cost efficient approach to mitigate legal risks will normally be to geographically delimit the marketing material, including especially access to enter contracts. In absence of international standards for defining the targeted states, businesses may want to divide their websites into different regions from which the user has to choose.[33] Thereby business can at least to some extent control whereto which material is disseminated.[34]

Systems for technical delimitation are possible to elaborate in a way that users from non-targeted states will not obtain access to the business' marketing material or specific parts thereof. This can be done if e.g. a country code is connected to the user information sent in Internet communication.[35] Such delimitation will probably be more effective than the above-mentioned solution

Another approach to cost-efficient legal risk management, which should be combined with geographical delimitation, is to adjust the marketing material in accordance with guidelines of international nature or national guidelines in the targeted states.[36] Guidelines are normally available on the Internet free of charge and are often unlike laws designed for practical implementation.

Guidelines are often less precise than the law itself but can at a relatively low cost provide valuable information on how to mitigate legal risks. Getting precise information about the law is normally an expensive and cumbersome process, which may be preferable for businesses that are more vulnerable to e.g. unfavourable commenting.[37]

---

32 The assessment should also comprise the cost connected to more severe punishment in the case of repeat offences.

33 Se e.g. www.sonyericsson.com, www.levis.com, www.mcdonalds.com

34 It will mainly be product information, offers and contracting ability that businesses should delimit, whereas general information about the business is less likely to give rise to problems.

35 See e.g. www.infosplit.com.

36 See e.g. the 1999 OECD guidelines for Consumer Protection in the Context of Electronic Commerce, www.oecd.org and a number of guides for both consumers and businesses at www.ftc.gov/bcp/menu-internet.htm. See also the 2002 Position Statement of the Nordic Consumer Ombudsmen on E-Commerce and Marketing on the Internet, www.fs.dk/uk/acts/nord_gui.htm.

37 Since there is some similarities in the law of regions, it may be more efficient to only obtain detailed legal information in a limited number of states.

12. Managing Cross-Border Law Enforcement

States may have to reconsider their law enforcement to match the international nature of the Information Society. States may want to use possibilities in domestication and privatising law enforcement along with applying alternative law enforcement. First of all states should however seek to minimize the need for cross-border law enforcement.

Laws containing behavioural norms are made on political grounds in order to protect the state as such, including its inhabitants. The purpose of law enforcement is to protect states from the damage caused by these undesirable acts. Law enforcement management is about optimizing compliance with the law by employing scarce enforcement resources.

Even though the Internet has opened up for new types of scam and other undesirable acts, the Internet has also provided law enforcers with new powerful tools for monitoring and investigating businesses' behaviours. Unlike traditional physical shops, shops on the Internet can be examined at a relatively low cost from the desk of a civil servant.[38]

Since businesses may be expected to have an interest in complying with the law of markets, which they addresses, a fundamental measure by the state should be to provide easy accessible information on how to comply with the law of that state. Equally important is information on which measures the business can take in order not to be considered to do business in that state.

Another preventive approach is to educate those inhabitants of the state who may suffer from illegal activities carried out by foreign businesses.[39] These preventive approaches can be carried out by the state and/or by private consumer or business organisations who also have an interest in confidence in electronic commerce.

Cross-border law enforcement is less cumbersome if carried out solely within the state's territory. States should therefore consider possibilities of prohibiting use of or contribution to illegal activities, including possibilities for users to seek redress through payment intermediaries.

States may also consider applying technical or market based alternative law enforcement. Both approaches entail concerns regarding fair trial, which may be ignored in a purely administrative process. Both approaches can be suitable for a number of enforcement purposes.

Establishing a system for technical based law enforcement (e.g. blocking) can be done in collaboration with access providers. Legal guarantees can e.g. be secured through a 'blocking-board' with legal experts and with possibilities of bringing the board's decisions before a court. A list of blocking orders can

38 This has e.g. been the case in connection to Sweep Days, carried out by the International Consumer Protection and Enforcement Network, where consumer organisations around the world has search for certain types of illegal business activities. See www.www.icpen.org.

39 See e.g. www.ftc.gov/bcp/menu-internet.htm.

regularly be disseminated electronically to mandatory filters in the access providers' systems.

Market based law enforcement is more indefinable and less predictable than technical enforcement. If states decide to apply information based public law enforcement, the state should also consider how to include legal guarantees and how to deal with situations where harm is caused to a business on groundless allegations.[40]

Except for clear offences, where expressing warnings or other strong attitudes may be appropriate, states should in order not to dilute the credibility of public authorities consider to only provide objective information and seek to educate people at a more general level. It is less problematic if private parties use the market for law enforcement under a possible liability for libel.

States may consider attaching civil sanctions to legislation such as unenforceability of contracts and compensation in connection with e.g. misleading advertising. Unenforceability in e.g. consumer contract may be effective in connection with imposing charge back obligations for payment intermediaries.[41]

If states already have established an enforcement system for civil judgements as the European system described above, civil tort sanctions may be more effective than sanctions under public law enforcement. States may in connection with a system where civil law suits are recognised in some foreign states consider how to improve such law enforcement through e.g. legal aid schemes.

13. International cooperation

Cross-border law enforcement can be further improved through international cooperation. Cooperation can be in the form of substantive harmonisation or procedural harmonisation, including investigation and mutual assistance. Such cooperation already exists on a regional level in many states.

One of the key attributes of alternative law enforcement is that the enforcing state does not need assistance by the state of the offender. On the other hand the states may have a common interest in cross-border trade, which may lead to establishment or widening of existing trade agreements.

Traditional cross-border law enforcement is easier and more cost-efficient to carry out in the state of the offender, where legal remedies can be applied under the sovereignty of that state. This however requires cooperation

40 In a recent incident, the Dutch Consumer Organisation, Consumentenbond, warned against buying Epson printers because of an alleged deceptive smart chip. The warning was later withdrawn after Epson managed to convince Consumentbond that the chip was not deceptive. See Cullen, Drew, Epson, We Don't Have a Problem, 20 July 2003, www.theregister.co.uk.

41 Payment intermediaries can benefit from a string of contracts leading back to vendor and the possibility of internalizing the 'enforcement costs'.

between the enforcing state and the state of the offender.

Cooperation on cross-border law enforcement is based on mutual trust and a common interest in effective law enforcement. Mutual trust is easier to achieve the more similar legal systems are or the more harmonised the concerned area is. Substantive harmonisation can support international procedural cooperation.

When sufficient mutual trust is established recognition of judgements or application of foreign law can be introduced in specific areas or in more general forms. States can consider including the principle of dual criminality along with more or less precise exception clauses including for grounds of public order. Procedural harmonisation can also consist of assistance in e.g. serving documents, investigation and the taking of evidence.[42]

Another approach is to attach international applicability to certain rules.[43] In this way states can ensure that businesses at least can be prosecuted in their country of establishment even though the action is directed towards other states. This principle may be efficient in connection to well-harmonised areas, whereas states' interest in forbidding actions, which are legal in the targeted state, may be rather limited.[44]

An issue that it is obvious to deal with at an international level is how businesses should delimit their marketing material in order to be in control of which states are being targeted and hence which laws to observe. A better solution may very well be found at a technical level, taking advantage of the nature of data communication on the Internet.

When it has been established how to divert marketing material on the Internet it will be less controversial to assist foreign states in the enforcement of their laws provided the business has directed its marketing material to that market. States can benefit from such agreements to the extent that they are based on reciprocity.

States should also at an international level consider how to provide easy access to legal information in different states. Private parties such as organisations or legal advisers may also provide this information. [45]

If possible at all, it will take a long time before traditional cross-border law enforcement can be carried out on a more international level. Meanwhile it may be beneficial to strengthen and widen the ongoing work on defining international standards for elaborating marketing material[46] and

---

42 See 2001 Council of Europe Budapest Convention on Cybercrime (ETS 185, 23 November 2001). See also Weber, Amalie M., The Council of Europe's Convention on Cybercrime, Berkely Technology Law Journal, No 1, Vol. 18, 2003, p. 425.

43 See the 2000 EU E-Commerce Directive article 3.

44 In the 2000 EU E-Commerce Directive international applicability is found in combination with principles of home country control and mutual recognition. Between other states or areas not equally harmonised, international applicability may not be a feasible solution.

45 In the 2000 EU E-Commerce Directive article 19(4) is it prescribed that EU Member States shall establish contact points, where businesses inter alia can obtain details on authorities, associations or organisations from which they may obtain further information or practical assistance.

46 In the 2000 EU E-Commerce Directive article 16 is it established that the Member States and the Commission shall encourage the drawing up of codes of conduct at a Community

establishing/enhancing international enforcement networks.[47]

level.

47 See e.g. International Consumer Protection and Enforcement Network, www.icpen.org, OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (June 11th 2003), www.oecd.org and the EU proposal for a Regulation on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws (COM(2003)443 final, 18 July 2003).