# Chapter 5
# SHOULD SELF-REGULATION BE THE STARTING POINT?

**Bert-Jaap Koops, Miriam Lips, Sjaak Nouwt, Corien Prins and Maurice Schellekens**

## 5.1 Introduction

In this chapter the concept of self-regulation will be discussed as the starting point in regulating ICT-related behavior. In his book *Self-Regulation in the Media Sector and European Community Law*, Jorg Ukrow defines self-regulation as follows: 'A regulatory activity carried out by specific organizational units in order to avoid or eliminate incorrect behavior within their internal structures, or within the structures from which they operate.'[1] We will take this definition as the working definition for our analysis of the starting point of self-regulation.

In its most extensive form, self-regulation implies that private actors themselves implement the applicable norms and rules and, ideally, monitor compliance and enforce the rules in case of non-compliance. Self-regulation is therefore often used as an argument in proposing a system that is different from formal regulation by national governments or international regulatory bodies.

However, many different forms of the concept emerged in the highly diverse areas in which self-regulatory initiatives have been implemented, varying from norms applicable to the environment, the media, and advertising, to diverse professional standards, such as those applied in the medical profession. As will be shown in this chapter, several of these forms play a role in the area of ICT as well. Some do not exclude government regulation, but are based on co-operation between official bodies and private actors. Forms are also available in which the general framework of norms has been established by means of legislation, but further details have been elaborated by the relevant sectors through, for example, codes of conduct.

Self-regulation is often embraced as a highly attractive alternative to regulation by means of laws and other legislative acts. Proponents of self-regulation complain, for example, about the lack of flexibility of legislation and are skeptical about the feasibility of efficient and adequate ICT regulation by means of legislation. However, various imperfections and adverse consequences for the Internet are at-

[1] Ukrow 1999, p. 12.

*B.-J. Koops, et al. (Eds), Starting Points for ICT Regulation*

tached to self-regulation and there is certainly reason to question the adequacy and effect of self-regulation in certain circumstances. For example, in their enthusiasm for self-regulation, proponents often seem to overlook the difficulties that arise in relation to the enforcement of self-regulatory initiatives. Furthermore, who may advocate a leading role for self-regulation and for what reasons? In ICT regulation, what strengths and weaknesses of self-regulation can be noted? Can criteria for ICT-related self-regulation be developed? These and many other questions are often ignored in the discussions on the role of self-regulation in the area of ICT.

The aim of this chapter is to show the complexity of the starting-point of self-regulation. In doing so, we will set the general stage for the discussion in the first part of this chapter. This analysis will start with a glance at the policy documents that make reference to self-regulation (section 5.2). Subsequently, we will analyze the meaning and types of self-regulation and its relationship with government regulation (section 5.3). In this section, the pros and cons of self-regulation will be addressed and several examples of self-regulatory initiatives to illustrate how they work in practice. In the second part of this chapter, we will present a more critical analysis of the concept of self-regulation. In section 5.4, criteria will be developed to decide when self-regulation should or should not be considered. To meet these criteria, various instruments will be available. We will focus in particular on the interaction between government and private action with respect to self-regulatory initiatives (section 5.5). We will finish by trying to define how and to what extent self-regulation should indeed be a starting point for ICT regulation (section 5.6).

## 5.2 Where Does It Come From?

In this section, we will pay attention to opinions about self-regulatory issues that can be found in policy documents. We will distinguish between opinions in policy documents at an international level, from international organizations and, at national levels in several countries. At the international level, many legal ICT-related questions have been addressed, for example, in the areas of network interconnection, intellectual property rights, information security, and privacy and personal data, and policy documents about such issues often voice support for self-regulation as a starting point (section 5.2.1). At a national level, we will focus on Australia, the Netherlands, the UK, and the US, as examples of countries that have called for self-regulation in various domains (section 5.2.2).

### 5.2.1 **International initiatives**

#### 5.2.1.1 *European Union*

At the European Ministerial Conference, jointly organized by Germany and the European Commission, which took place in Bonn on 6-8 July 1997, the participat-

ing ministers drafted a declaration with starting points to identify barriers to the use of Global Information Networks, with possible solutions, and a call for an open dialogue on further options for European and international co-operation.[2] In Recommendation 19, the Ministers declared that self-regulation can be a useful instrument to regulate behavior in a Global Information Network: 'Ministers stress the role which the private sector can play in protecting the interests of consumers and in promoting and respecting ethical standards, through properly-functioning systems of self-regulation in compliance with and supported by the legal system.'

On 25 January 1999, the European Parliament and the Council adopted a multi-annual Community action plan, following-up on a European Commission's Green Paper of 23 October 1996, on promoting safer use of the Internet by combating illegal and harmful content on global networks.[3] In Article 3, the decision promoted industry self-regulation and content monitoring schemes, for example, dealing with content such as child pornography or content which incites hatred on grounds of race, sex, religion, nationality, or ethnic origin. Furthermore, industry was encouraged to provide filtering tools and rating systems, which would allow parents or teachers to select content appropriate for children in their care while allowing adults to decide what legal content they wish to access, and which take account of linguistic and cultural diversity.

In 2001, in a white paper called *European Governance*,[4] the European Commission focused on the way in which the Union uses the powers given by its citizens. The Commission is of the opinion that reform should start, so that the citizens see changes well before further modification of the EU Treaties. The White Paper proposed changes in the policy-making process to get more people and organizations involved in shaping and delivering EU policy. It promoted greater openness, accountability, and responsibility for all those involved, to show citizens how the Member States, by acting together with the EU, can to tackle their concerns more effectively.

The Commission proposed changes for 'better policies, regulation and delivery'. In this context, the Commission declared that it would promote greater use of different policy tools: regulations, framework directives, and co-regulatory mechanisms.

One of the factors that, according to the Commission, can improve the quality, effectiveness and simplicity of regulatory acts, is a framework of co-regulation. The use of co-regulation can be an effective way of achieving EU objectives: 'Co-regulation implies that a framework of overall objectives, basic rights, enforcement

---

[2] European Commission, *Ministerial Declaration*, Ministerial Conference, Bonn, 6-8 July 1997, <http://europa.eu.int/ISPO/bonn/Min_declaration/i_finalen.html> (last visited 10 February 2005).

[3] Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999, adopting a multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. OJ, 6.2.1999, L 33/1.

[4] European Commission, *European Governance. A White Paper*, Brussels, 25.7.2001, COM (2001) 428 final, < http://europa.eu.int/eur-lex/en/com/cnc/2001/com2001_0428en01.pdf>.

and appeal mechanisms, and conditions for monitoring compliance is set in the legislation.'[5]

Co-regulation should combine binding legislative and regulatory action with actions taken by the actors most concerned, drawing on their practical expertise. Involving the stakeholders most affected creates a wider ownership of the policies, and this should result in better compliance, even where the detailed rules are non-binding. The Commission points at the internal market, where co-regulation has already been used (the 'New Approach' directives), and at the environment sector (reducing car emissions). The exact way in which legal and non-legal instruments are combined and the actor who launches the initiative (the Commission or stakeholders) will vary from sector to sector.

Furthermore, in the context of the EU's contribution to global governance, the Commission was convinced that, for example, the development of co-regulatory solutions to deal with aspects of the new economy could be tested at a global level. The Commission believed that, as in the EU, these approaches should complement successful elements of international public law, most notably the World Trade Organization and the International Court of Justice.[6]

On 28 May 2002, the European Commission presented a Communication entitled 'e-Europe 2005: An Information Society for All'. This Communication was an action plan presented in view of the Sevilla European Council on 21-22 June 2002. In this action plan, the European Commission stressed the initiative to promote self-regulation in the information society. The Commission stated that, since the publication of the e-Commerce Communication in 1997,[7] it had developed a comprehensive policy in this field. Among the achievements were a series of directives[8] aimed at establishing an Internal Market for information society services, as well as a number of non-legislative initiatives aimed at promoting self-regulation, notably in the field of 'e-Confidence' and On-line Dispute Resolution (ODR),[9] and the launch of the 'Go Digital' initiative to help small and medium-sized enterprises to improve e-Business use.

#### 5.2.1.2 *OECD*

On 16-17 February 1998, the Organization for Economic Co-operation and Development (OECD) organized a workshop, with the support of the Business and In-

[5] Ibid.

[6] Idem, p. 27.

[7] A European Initiative in Electronic Commerce, COM (1997) 157 final of 16.4.1997.

[8] Directive 2000/31/EC on electronic commerce, Directive 1999/93/EC on a Community framework for electronic signatures, Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the Information Society, Directive 97/7/EC on the protection of consumers in respect of distance contracts.

[9] The Commission has established an alternative dispute settlement network, the EEJ net, in order to utilize and promote dispute resolution mechanisms for resolving cross-border consumer-business disputes throughout the EU.

dustry Advisory Committee (BIAC), which brought together representatives of governments, the private sector, user and consumer communities, and data protection authorities. They considered issues linked to the protection of privacy and transborder flows of personal data in the developing global networked society and examined how the OECD Privacy Guidelines may be implemented in the context of global networks. The OECD tried to find mechanisms and technological tools that could provide an effective bridge between the policies for protection of personal data offered by the legislators in the European Union and the policies of other Member countries aimed at encouraging the private sector to provide meaningful protection for personal data on global networks by effective self-regulation. The workshop sessions addressed the following issues:

- identifying and balancing the needs of the private sector and those of users and consumers and formulating efficient strategies for 'educating for privacy';
- developing privacy-enhancing technologies;
- implementing enforcement mechanisms developed in the private sector for privacy codes of conduct and standards;
- adopting model contractual solutions for transborder data flows.

At the end of the workshop, the chair, Michelle d'Auray (Electronic Commerce Task Force, Industry Canada), highlighted the need to survey the instruments available for data protection, including law, self-regulation, contracts, and technology, in order to assess their practical application in a networked environment and their ability to meet the objectives of the OECD Privacy Guidelines, for example, effectiveness, enforceability, redress, and coverage across jurisdictions.

On 7-9 October 1998, the OECD Ministers present at the Ottawa Conference 'A Borderless World: Realizing the Potential of Global Electronic Commerce' issued a declaration on behalf of the governments of the OECD Member Countries, including the European Communities.[10] The Ministers:

> 'will take the necessary steps, within the framework of their respective laws and practices, to ensure that the OECD Privacy Guidelines are effectively implemented in relation to global networks, and in particular:
> 1. encourage the adoption of privacy policies, whether implemented by legal, self-regulatory, administrative or technological means;
> 2. encourage the on-line notification of privacy policies to users;
> 3. ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress;
> 4. promote user education and awareness about on-line privacy issues and the means at their disposal for protecting privacy on global networks;

[10] OECD, Ministerial Declaration on the Protection of Privacy on Global Networks, DSTI/ICCP/REG(98)10/FINAL. On the Internet: <http://www.oecd.org/dataoecd/39/13/1840065.pdf>.

5. encourage the use of privacy-enhancing technologies; and
6. encourage the use of contractual solutions and the development of model contractual solutions for on-line transborder data flows.'

The Ministers invited relevant international organizations to take the Declaration into consideration as they develop or revise international conventions, guidelines, codes of practice, model contractual clauses, technologies and interoperable platforms for protection of privacy on global networks. Industry and business were invited to take account of the objectives of this Declaration and to work with governments to further the objectives by implementing programs for the protection of privacy on global networks.

In general, all work that the OECD has done in the area of privacy[11] suggests that it considers the most effective privacy protection on-line likely to be delivered through a mix of regulatory and self-regulatory approaches, blending legal, technical, and educational solutions that suit the legal, cultural, and societal context in which it operates. According to the OECD, statutory systems can be more effective while using the wide range of self-regulatory measures to implement and enforce law on-line. On the other hand, self-regulation will also be more effective when it is backed-up with appropriate legislation and effective government enforcement. Enforceability is crucial because it may not be assumed that there will be compliance with either system.

#### 5.2.1.3 *UN/ITU*

On 10-12 December 2003, the International Telecommunication Union (ITU) in Geneva organized the first phase of the World Summit on the Information Society (WSIS). This world summit was endorsed by the General Assembly of the United Nations.[12] The ITU is the UN agency that holds the leading role in the organization of WSIS. The summit addressed a broad range of themes concerning the information society, and a Declaration of Principles and a Plan of Action were adopted. The second meeting will be held at Tunis in November 2005.

In the Declaration of Principles, key principles for building an inclusive information society were outlined,[13] one of these being an enabling environment. In this context, the Declaration of Principles states that:

**check!**

'The rule of law, accompanied by a supportive, transparent, pro-competitive**Fout! Bladwijzer niet gedefinieerd.**, technologically neutral and predictable policy and regulatory framework reflecting national realities, is essential for building a people-

[11] See also the OECD report *Privacy On-line: Policy and Practical Guidance*, 21 January 2003, <http://www.olis.oecd.org/olis/2002doc.nsf/LinkTo/dsti-iccp-reg(2002)3-final>.

[12] Resolution 56/183 (21 December 2001).

[13] World Summit on the Information Society, *Declaration of Principles*, Document WSIS-03/GENEVA/DOC/0004 (12 December 2003), available at <http://www.itu.int/wsis/documents/>.

centered Information Society. Governments should intervene, as appropriate, to correct market failures, to maintain fair competition, to attract investment, to enhance the development of the ICT infrastructure and applications, to maximize economic and social benefits, and to serve national priorities.'

Furthermore, within the context of the key principle to create an enabling environment, the Declaration of Principles pays attention to governance issues and also leaves room for self-regulation:

'The management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that:
a) Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues;
b) The private sector has had and should continue to have an important role in the development of the Internet, both in the technical and economic fields;
c) Civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role;
d) Intergovernmental organizations have had and should continue to have a facilitating role in the coordination of Internet-related public policy issues;
e) International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.'

Thus, it appears that governance is a joint effort of public and private parties. 'Governments, as well as private sector, civil society and the United Nations and other international organizations have an important role and responsibility in the development of the Information Society and, as appropriate, in decision-making processes.' There should be 'a mechanism for the full and active participation of governments, the private sector and civil society from both developing and developed countries, involving relevant intergovernmental and international organizations and forums, to investigate and make proposals for action, as appropriate, on the governance of Internet by 2005.'[14]

### 5.2.2 **National initiatives**

#### 5.2.2.1 *Australia*

In August 2000, the Australian Taskforce on Industry Self-Regulation published their policy document *Industry Self-Regulation in Consumer Markets*.[15] The Taskforce was established in August 1999 by the then Minister for Financial Ser-

[14] Ibid.
[15] Available on the Internet: <http://www.selfregulation.gov.au/publications/TaskForceOnIndustrySelf-Regulation/FinalReport/contents.asp>.

vices and Regulation, Joe Hockey. It reported to the Government in August 2000 following two rounds of consultation with business and consumer representatives all around Australia. The report outlines the nature and extent of self-regulation in Australia and sets out good-practice principles for self-regulatory schemes.

On 13 December 2000, the Minister for Financial Services and Regulation announced the publication of a guideline for businesses, consumers, and government advisers. This guideline, which is currently being drafted, is intended to provide practical advice on self-regulation and to be a gateway to other resources on self-regulation.[16]

In its report, the Taskforce describes how self-regulatory schemes can promote good practices and target specific problems within industries. These schemes can force lower compliance costs on business, and offer quick, low-cost dispute resolution procedures. They can also avoid the often overly prescriptive nature of regulation and allow industry the flexibility to provide greater choice for consumers and to be more responsive to changing consumer expectations.

The Taskforce gave two general recommendations. First, it encouraged the government to provide industries with further practical guidelines, based on the principles in their report, for the development and review of self-regulatory schemes. Second, it recommends the government to update its guidelines for policy makers on how to assess the range of options for addressing a particular market failure or social policy objective. By doing so, the Taskforce findings can be incorporated in the industry environment and market circumstances that are most likely to lead to effective self-regulation.

In its report, the Taskforce concluded, furthermore, that there is no one model for self-regulation. Nevertheless, it identified the following common characteristics, called principles:

- The appropriate form of self-regulation will depend on what is to be achieved – that is the way in which it is necessary to significantly improve market outcomes for consumers. This can vary within and between industries.
- The form of self-regulation adopted by industry should be one that effectively solves the identified problem and minimizes costs for industry.
- The type of dispute resolution scheme, if required, should depend on the nature of the complaints and type of self-regulatory model.
- A scheme is only as effective as its broader coverage of industry participants, so it should aim for comprehensive membership.

#### 5.2.2.2 *The Netherlands*

At a national level, in the Netherlands, the importance of self-regulation has been stressed several times. In the 1998 policy document *Legislation for the Electronic*

[16] *Industry Self-Regulation – A how to guide*, <http://www.selfregulation.gov.au/ind_self_reg.asp>.

*Highways*,[17] some preference was voiced for self-regulation. According to the Dutch Guidelines for regulation [*Aanwijzingen voor de regelgeving*],[18] government legislation is only allowed when action by the central government is necessary, and when self-regulation is expected to yield insufficient results. Dematerialization, internationalization, and technological turbulence make this criterion even more important within the electronic environment. Within such a technically complex and international environment, social organizations sometimes have more expertise and knowledge of sector-specific problems and of the feasibility and adequacy of possible solutions than the government. Besides, self-regulation is not restricted to the territorial borders of a country.[19]

The Dutch government stresses that, in self-imposed standards, adequate attention should be paid to different interests, especially those of vulnerable parties. Also, the enforcement of the standards should be trustworthy. It is the government's duty to ascertain compliance with these conditions. However, the scope of self-regulation is restricted: self-regulation is not suitable for regulating the fundamental principles of the constitutional state. In that case, government itself needs to regulate.[20]

In the policy document *Internationalization and Law in the Information Society* (2000), the Dutch government formulated the following: 'The aim is to develop co-regulation and to stimulate self-regulation at an international level.' The Dutch government gave high priority to the development of co-regulation and to the stimulation of international self-regulation for the on-line environment.[21]

#### 5.2.2.3 *United Kingdom*

In December 2001, the British government published a policy document entitled *E-Policy Principles*.[22] Like many others, the British government wants to make its country one of the world's leading knowledge economies. To that end it wants to provide an effective 'light-touch' regulatory regime for the UK to engage in e-commerce and use the Internet safely and securely. The policy framework aims to ensure consumer confidence and trust in e-commerce and the use of the Internet. The e-policy principles are addressed to all policy makers working on proposals that may affect the Internet and e-commerce (see also chapter 1 of this Volume). They are designed to make policy makers aware of the impact that local, national, European and other international policy decisions and legislative proposals may have on e-commerce.

---

[17] See LEH Memorandum 1998, in Dutch: Kamerstukken II, 1997-1998, 25 880, nos. 1-2.
[18] See Aanwijzingen voor de regelgeving, Stcrt. 26 November 1992, 230 (in Dutch).
[19] See *supra* n. 17, at pp. 180-181.
[20] Ibid.
[21] ILIS Memorandum 2000.
[22] UK e-Government Unit, *The Principles of e-Policy Making*, <http://e-government.cabinet office.gov.uk/assetRoot/04/00/60/79/04006079.pdf>.

One of the eight e-policy principles deals with self-regulation: 'Consider self and co-regulation options.' This principle means that to encourage trust and the fast, effective resolution of problems, the Government is pursuing a policy of promoting co-regulation between providers, users, and regulators. The British government sees its role as defining goals from a public-interest perspective and ensuring that there is an adequate and up-to-date framework of law where necessary. If possible, the Government will look at providers and users and stimulate non-legislative arrangements like codes of conduct, guidelines, and voluntary schemes for dispute resolution. In general, such arrangements provide a more rapid and flexible answer to changing market needs and achieve more international consensus than is possible through legislation. However, the Government warns that self-regulation or co-regulation is not a cost-free option.

#### 5.2.2.4 *United States*

In the earlier years of Internet regulation, the US government indicated a strong preference for self-regulation, particularly in the area of commerce. The very first principle of the White House's 1997 *Framework for Global Electronic Commerce* is headed: 'The private sector should lead':

> 'Though government played a role in financing the initial development of the Internet, its expansion has been driven primarily by the private sector. For electronic commerce to flourish, the private sector must continue to lead. Innovation, expanded services, broader participation, and lower prices will arise in a market-driven arena, not in an environment that operates as a regulated industry.
> Accordingly, governments should encourage industry self-regulation**Fout! Bladwijzer niet gedefinieerd.** wherever appropriate and support the efforts of private sector organizations to develop mechanisms to facilitate the successful operation of the Internet. Even where collective agreements or standards are necessary, private entities should, where possible, take the lead in organizing them. Where government action or intergovernmental agreements are necessary, on taxation for example, private sector participation should be a formal part of the policy making process.'[23]

**check!**

The same approach was taken by the Department of Commerce:

- Governments must allow electronic commerce to grow up in an environment driven by markets, not burdened with extensive regulation, taxation or censorship. While government actions will not stop the growth of electronic commerce, if they are too intrusive, progress can be substantially impeded.
- Where possible, rules for the Internet and electronic commerce should result from private collection action, not government regulation.

---

[23] The White House, *A Framework for Global Electronic Commerce*, 1 July 1997, <http://www.technology.gov/digeconomy/framewrk.htm>.

However, there is a role for the government in providing a legal framework:

- Governments do have a role to play in supporting the creation of a predictable legal environment globally for doing business on the Internet, but must exercise this role in a non-bureaucratic fashion.[24]

Several American agencies give attention to self-regulation. An example is the Federal Trade Commission (FTC), which addresses various issues related to regulatory problems in the area of electronic communications, such as fraud on the Internet, buying on-line, spamming, and Internet auctions. In July 2000, the FTC published a report on On-line Profiling, in which it supported an industry plan drafted by the Network Advertising Initiative (NAI),[25] to self-regulate consumer privacy protection in this area. However, at the same time, the FTC concluded that legislation seemed necessary to enforce the industry guidelines.[26]

It seems that, over the years, the US has gradually shifted from vehemently stressing self-regulation as a starting point to a more nuanced point of view, in which government regulation is increasingly seen as a useful tool in ICT regulation. In fact, 'the end of self-regulation' may even be discerned when looking at the host of regulatory initiatives the US has taken in the past few years in the area of ICT.[27]

## 5.3 What Does It Mean?

### 5.3.1 **Key characteristics**

We started this chapter by introducing the concept of self-regulation by presenting Jorg Ukrow's definition. Many other definitions have been suggested, but we are not concerned here with a precise definition. For the purpose of this chapter, a brief discussion of the key characteristics of the concept will suffice.[28] In general, self-regulation could be described as the regulation and co-ordination of behavior (of

---

[24] Department of Commerce, *The Emerging Digital Economy*, April 1998, p. 50, < http://www.technology.gov/digeconomy/EmergingDig.pdf>.

[25] The Network Advertising Initiative (NAI), a coalition of America's largest profile marketers, authored an industry plan, the NAI guidelines, and established a basic set of rules for notice of on-line information collection activities, consumer consent to such information collection and future marketing uses, consumer access to information held by on-line marketers, and security protection with respect to such information.

[26] Federal Trade Commission, *On-line Profiling: A Report to Congress. Part 2: Recommendations*. July 2000, <http://www.ftc.gov/os/2000/07/on-lineprofiling.htm#III.%20RECOMMENDATIONS>.

[27] Geist 2003, p. 351.

[28] For a more detailed analysis of self-regulation, see Baldwin & Gave, 1999, in particular, Chapter 10.

individuals or groups) through rules of societal organizations or through the application, compliance checking and enforcement of those rules.[29] There may or may not be a specific legal basis for those rules.

Self-regulation can therefore be characterized through its constituent elements, such as self-rule-making, self-jurisdiction, and self-enforcement. Self-rule-making indicates that the interest groups, social organizations, or stakeholders themselves draft the rules. This may imply that one interest group or organization draws up the rules, but it is also possible that several groups representing different interests formulate the rules together. The rules that eventually come about are applicable to the members of the interest group or social organization that has drafted the rules (self-jurisdiction). If the rules are binding for the members, such bindingness is often based on an agreement to abide by such rules. Finally, the group or the organization may take measures against those members that do not abide by the rules in order to make sure that they do so henceforward (self-enforcement). Self-enforcement may also involve the monitoring or supervision of adherence to the rules in order to detect possible breaches of the rules.

### 5.3.2 Typology and the relation to government regulation

Self-regulation is often contrasted with government regulation. The most prevalent and typical form of government regulation is legislation. Legislation is the result of a democratic process on a constitutional basis by which rules are enacted that are binding on the territory of the pertinent state, and these rules are binding precisely because of the very procedure by which they came about. The above definition perhaps suggests that self-regulation and government regulation are two distinct and mutually exclusive, alternative forms of regulation. From an analytical perspective, this may very well be true but, in practice, government legislation and self-regulation are often each other's complement in the regulation and co-ordination of behavior. In literature, much attention has been paid to the relation between self-regulation and legislation, and a number of basic forms of self-regulation have been distinguished, based on their relation to government regulation: pure self-regulation, proxy self-regulation, legally stipulated self-regulation, and co-regulation.

In the case of pure self-regulation,[30] the initiative for self-regulation rests fully on the interest group. Government remains neutral to the outcome of their initiatives. Of course, the rules thus drafted may not contravene existing national legislation. Examples of pure self-regulation are domain-name dispute resolutions mechanisms, such as ICANN's UDRP,[31] or standards, for example, the Model Code for the Protection of Personal Information, approved as a 'National Standard of Canada' by the Standards Council of Canada.[32]

---

[29] Eijlander 1994, p. 94.
[30] Eijlander & Voermans 1999, p. 71.
[31] See <http://arbiter.wipo.int/domains/>.
[32] Bennett & Raab 2003, p. 127.

Proxy self-regulation is accomplished without an explicit obligation to do so, except where government puts pressure on interest groups to realize self-regulation. Because public interests may be at stake, the government guards over these interests in the background. An example of proxy self-regulation is a code of conduct about mergers and takeovers in the (newspaper) publishing business, for example, to prevent an oligopolistic market structure.[33] Such an implicit threat of government regulation may also very well have been an important factor in the establishment, in the later 1990s, of Internet hotlines for illegal and harmful content. At the time, ISP liability was still very much in discussion; content issues may well have tipped the balance towards a stricter liability for Internet Service Providers. Thus, for instance, Dutch ISPs took the initiative to create a Dutch hotline for child pornography; they wanted to be seen doing something against child pornography on the Internet.

Pure self-regulation and proxy self-regulation do not *as such* fall within a legal framework. Types of self-regulation that are being accomplished within an existing legal framework are called stipulated self-regulation.[34] Legally stipulated self-regulation can be characterized as follows: the legislature sets the framework conditions within which the self-regulation has to be accomplished. Within the framework, citizens, companies, and social organizations have considerable freedom in drafting their rules. However, government has a more active role than with pure or proxy self-regulation. The ways and extent of stipulated self-regulation may differ. The legislator can merely prescribe the procedure for the realization of self-regulation and, for example, make provisions for dispute resolutions. In other cases, the legislator can also prescribe conditions for the results of the self-regulation, or the legislator can prescribe the minimum issues that have to be regulated.

Three types of stipulated self-regulation can be distinguished, according to the types of legislation that support self-regulation.

1. *A statute attaches legal consequences to self-regulation*. The legislator may oblige a certain group to draft self-regulation and stipulate what legal consequences are attached to the self-imposed rules, to what legal issues the self-regulatory rules are applicable, or what the legal status is of enforcement or other decisions of a self-regulatory body. It is, possible, for example, to obtain a legal order with which a decision of a self-regulatory body can be executed. Disciplinary law is but one example of this type of self-regulation.
2. *A statute prescribes procedures for self-regulation and for the legal consequences of the self-regulation*. Sometimes, the legislator offers the possibility to generate self-regulation, according to a specific procedure. As a result, the drafted self-regulation results in legal consequences. An example is the drafting of codes of conduct on data protection in a certain sector. Various Data

[33] See *supra* n. 30, at, p. 72.
[34] Ibid.

Protection Acts in Europe, following the Directive on the protection of personal data, allow Data Protection Authorities to declare that the code of conduct conforms with the law, thus giving legal effect to the code, but only if certain procedural criteria are met, such as sufficient representation (see also section 5.4.2).

3. *A statute lays the foundation for new legislation if self-regulation is not forthcoming*. Sometimes, the law makes a provision for legislation, for situations where self-regulation is not achieved or does not measure up. An example of this is the DRM provision about Digital Rights Management (hereinafter: DRM) in the Copyright Harmonization Directive:[35] 'In the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that right holders make available to the beneficiary of an exception or limitation provided for in national law.'[36] That is, if industry self-regulation does not sufficiently safeguard the interests of users of copyrighted material to benefit from the legal exceptions to the copyright, states should enact legislation to safeguard those rights. Another example is the statement of the Joint Committee on the British Draft Communications Bill, which noted that the Office of Communications (OFCOM), the communications regulator which was created by the Communications Act, should retain back-stop powers and the statutory right to re-impose detailed regulation where self-regulation fails to comply with agreed standards.[37]

Although the extent of stipulated self-regulation may vary, there is a difference between self-regulation and legislation with open norms or vague rules. By using open norms, the legislator leaves the specific interpretation and effects of the legal framework to the addressee and in last resort to the courts. This does not have to result in self-regulation.[38]

Finally, co-regulation is a kind of regulation that is characterized by the co-operation between government and the private sector. Government and social organizations are equal partners in initiating discussions about social problems and solving them. Co-regulation is a communicative way of decision-making, where the government is not the central actor who defines problems and initiates solutions. It is a kind of policy-making with open negotiations between interested parties about the nature, the extent, and the seriousness of certain problems and the directions and options for solution.

---

[35] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, OJ L 167/10, 2001.

[36] Art. 6 para. 4 Directive 2001/29/EC, OJ L 167/10, 22.6.2001.

[37] Joint Committee Report, para. 71. See McKean & Hinton 2002.

[38] See *supra* n. 30, at p. 74.

As ICT law advances through the years, a gradual increase can be discerned in preference for co-regulation. In a 2000 inventory of government positions on ICT regulation,[39] we concluded that co-regulation is prominently present in several policy documents across Europe, at least in the Netherlands, Germany, France, and the United Kingdom, relating to e-Commerce and Internet policy. In 2001, in the European Commission White Paper on European Governance,[40] the Commission clearly saw a role for co-regulation, but would only allow this instrument to be used if certain conditions were met (see sections 5.2.1.1 and 5.5). Even in the US, there is a tendency to think that government should play a more important controlling part in realizing ICT policy, together with the industry and other social organizations. The OECD has also shown appreciation for co-regulation.[41]

### 5.3.3 **Advantages and disadvantages of self-regulation**

It is clear that self-regulatory initiatives have both strengths and weaknesses. In general, the advantages of self-regulation appear to be efficiency, flexibility, an incentive for compliance, and reduced costs for government. American scholars in particular have paid considerable attention to the benefits of self-regulation, given that private ordering is considered, in the US, to be 'politically more attractive than new government regulation in this modern era of hostility towards the state.'[42] Hence, the concepts of 'private' and 'public' ordering in relation to the on-line world have been extensively explored and discussed.[43] Here, we briefly touch upon the key arguments in favor of self-regulation.

Drafting and adapting the rules is often less time-consuming when this is done through self-regulation than by drafting and implementing legislation. For with self-regulation, the process of setting the rules draws on the specific expertise of the actors involved. Also, the rules usually evolve gradually. The effect of this appears, among other things, that the drafting process of self-regulatory mechanisms is usually not surrounded by intense lobbying as is the case with the development of legislation and international rules. Noteworthy is also that the rules established through self-regulatory instruments are not externally imposed and monitored by actors unfamiliar with the specifics of the context. Instead, the rules build on values that are internalized, meaning that the relevant parties are often already familiar with them. Given the absence of time-consuming formal procedures, it allows for easy adaptation to changing circumstances, new expertise, and changed views as regards the values, the monitoring options, and the enforcement mechanisms. Thus, self-regulation can turn out to be more efficient and flexible than legislation.

---

[39] Koops, et al., 2000.
[40] See *supra* n. 4.
[41] OECD Forum on Electronic Commerce, *Report on the Forum*, Paris, 12-13 October 1999, p. 11.
[42] Lemley 2000, p. 1546.
[43] See for an extensive discussion: Radin & Wagner 1998.

Another advantage relates to the above-mentioned internalized values on which self-imposed norms are often built. It is the very essence of self-regulation that the norms incorporated in the self-defined standards reflect the standards of the relevant group. Thus, since the parties involved in self-regulation have drafted the rules themselves, or close representatives have done so, there is usually substantial commitment among parties to observe their own rules. This works as an incentive for compliance.[44] Moreover, the adoption of self-defined standards could raise awareness among the partners. It is also relevant here that the rules established by the group itself may be more specific than laws issued by national or international governments. The participants in the self-regulatory scheme are likely to be more willing to comply with rules to which they themselves contributed than if the rules were addressed at a distant level by political motivations.

A further advantage of self-regulation is that the costs of self-regulation are low for government. Self-regulation leads to costs for the parties involved in complying with their rules. Government can supervise the performance of self-regulation, but those costs will in general be much lower than the costs for regulating the market.

Finally, it has been contended that self-regulation is more consistent with the specifics of the Internet architecture, i.e., an environment which tends to defy centralized control.[45] The characteristics of the on-line world make it difficult for governmental authorities to regulate and control this world. Moreover, it is argued that: 'preserving autonomy in cyberspace helps to maintain a critical balance of power between the public and private sectors, that serves the common good. The more on-line regulations we have, the greater the state's influence in the affairs of cyberspace, and this will inevitably mean more centralized structures of choice.'[46]

Of course, self-regulation does not only have advantages. A prominent weakness of self-regulation is that, in principle, the rules can be revised at will, and little is guaranteed. In other words, the flexibility for changing the rules may simultaneously be a disadvantage. In addition, there may be a lack of transparency. Where procedures exist for the publication of legislation, such procedures usually do not exist for self-regulation. At least, it seems more difficult for citizens to know of the creation, existence, and monitoring of self-regulatory schemes. Thus, the advantage that rules are based on internalized values may also be counter-productive because of a lack of external accountability for these values. The values may turn out to be selective or too narrow-minded, in that they fail to recognize other (societal) values. A consequence of self-regulation may also be that the power of the strongest or best-organized participating party will increase. This may turn out nega-

---

[44] The EU White Paper on Governance states about co-regulation: 'The result is wider ownership of the policies in question by involving those most affected by implementing rules in their preparation and enforcement. This often achieves better compliance, even where the detailed rules are non-binding.' European Commission, *European Governance. A White Paper*, Brussels, 25.7.2001, COM (2001) 428 final, <http://europa.eu.int/eur-lex/en/com/cnc/2001/com2001_0428en01.pdf>.

[45] See, for example, Spinello 2001, p. 167.

[46] Ibid., p. 168.

tively for other participants. Here, the lack of democratic control appears to be a disadvantage. Proper or legitimate use of the self-regulatory mechanism would therefore require that rules are set for the administration of the mechanism (for example, a trustmark) and that these rules are made publicly available. After all, only with such a transparency might people disadvantaged by the scheme be able to set matters right by recourse to the courts.

Another weakness may be the mechanisms' lack of clarity. As mentioned, the instrument of self-regulation allows for more open norms than is the case with legislation. The consequence of this could be that the rules set remain rather vague and unclear for the citizens and businesses. Often, no transparent criteria exist to offer guidance for being able to genuinely trust self-regulatory schemes. Especially when schemes originate from different countries, the lack of clarity could mean that no common guidelines exist for assessing the merits of the schemes or for monitoring and enforcing the standards set. Given the borderless context of the on-line world, this concern is of particular importance.

When considering the problems and promises of self-regulation, it is worth looking at the results of a study conducted by researchers from Oxford University. The study shows that most successful self-regulatory activity has taken place where there is a clear legal basis, such as in the field of illegal content on the Internet. Self-regulation therefore seems to have been less successful where public policy objectives are less clear, for example, in relation to trust of Internet content. Moreover, the study points out that there are significant problems with many existing self-regulatory models including:[47]

- a lack of clarity and transparency about key processes, such as rating of material;
- procedures of code renewal and revision;
- insufficient transparency and accountability in code production processes;
- a lack of sustainability of funding of self-regulatory initiatives; and
- a lack of knowledge by those who are subject to a specific self-regulatory model like codes of practice.

Unfortunately so far, not much empirical research data have been available on user experience, trust, and perception of self-regulatory activities. As a result, it is difficult to assess the effectiveness of self-regulatory models and activities compared to for instance other regulatory alternatives, or to evaluate their impact on social processes. The Oxford study generally observes that, according to available studies on user attitudes towards the Internet, trust seems to be static or even declining. Although the Internet is increasingly used for all kinds of activities (e-commerce, e-learning, entertainment, information, friendships, different forms of community

[47] PCMLP, *Self-Regulation of Digital Media Converging on the Internet: Industry Codes of Conduct in Sectoral Analysis*, 30 April 2004, University of Oxford, <http://www.selfregulation.info/iapcoda/0405-iapcode-final.pdf>, last visited October 2004.

building, etc.), user trust in this medium seems to be affected by software viruses, unsolicited e-mail (spam), inappropriate or harmful contact and content, threat of prosecution for breach of copyright, and even criminal activities on-line.[48] Moreover, user knowledge on trustmarks provided by self-regulatory bodies turns out to be very low in Europe: only 10 per cent of EU citizens in 2003 were aware of trustmarks.[49] Most EU citizens also do not know where to report potentially harmful content: 57 per cent of EU citizens do not know whom to contact and only 13 per cent are aware of a self-regulatory solution like an ISP or hotline, with the Dutch citizens highest at 26 per cent.[50]

### 5.3.4 **Self-regulation in practice: How does it apply?**

Having discussed some theoretical dimensions of self-regulation in the area of ICT, it is interesting to take a brief glance at the initiatives that have been established thus far, since the above discussion might give the impression that the field of self-regulation is neatly structured and transparent. In practice, however, initiatives diverge in territorial scope, in the groups to which they are applicable (certain industry sectors, or whoever wants to participate), the parties that set up and run the self-regulatory scheme (industry or consumer associations, individual companies), the character of those parties (not-for-profit or commercial), and the scope as regards the subjects covered (single-issue or multiple-issue schemes). It is outside the scope of this chapter to provide even a very general overview of all the initiatives that have emerged over the years. Nevertheless, to give an impression, we will give a few examples in the next section that show a range of initiatives and characteristics present in different forms of self-regulation.

#### 5.3.4.1 *Codes, guidelines, and assessment schemes for on-line activity*

Self-regulatory instruments like codes of conduct, guidelines, seal programs, and voluntary schemes for dispute resolution usually have been created with the aim to regulate behavior in e-commerce environments. In several cases, they can be found in on-line public environments as well. In the last decade, many applications of these specific forms of self-regulation have seen the light.

A self-regulatory instrument frequently used by organizations is a code of conduct, a set of rules providing guidance on correct procedure and behavior for individuals. A well-known example the Code of Conduct for e-Commerce drafted by the Dutch Electronic Commerce Platform (ECP.NL).[51] This Code of Conduct has

---

[48] <www.selfregulation.info>, reporting of June 2004, p. 4, last visited October 2004.

[49] Eurobarometer 2004.

[50] See *supra* n. 47.

[51] In October 2001, a new version 4.0 of the Model Code of Conduct was published. See also ECP.NL, *Model Code of Conduct (Draft 4.0 2001),* <http://www.ecp.nl/ENGLISH/publication/cocdraft4.0ENG.pdf>. The standards outlined in version 3.0 were drafted after consultation with Dutch

become a model for international organizations such as the Organization for Economic Co-operation and Development (OECD) and the United Nations (UN).[52] The object of this Model Code of Conduct is to create trust in electronic commerce by incorporating major principles in the code, such as reliability, transparency, confidentiality, and privacy. The Model Code of Conduct may serve as a checklist to assess the degree to which contracts, general terms and conditions, regulations, etc., help to increase mutual trust in e-business, but may also be perceived as an example or a source of inspiration for organizations in drafting codes of conduct for e-business.

Available at many web sites nowadays, privacy codes are another example of self-regulatory instruments. Based on generally acknowledged information privacy principles, these codes contain a set of rules to be followed by organization members or users of websites concerned. Specific examples of these privacy codes can be found for companies (for example, American Express), sectors or industry associations (for example, the Federation of European Direct Marketing Associations), organizational practice (for example, direct marketing associations), technology, (for example, smart card technology) and professional societies (for example, librarians).[53]

Web sites that require high levels of trust, such as those concerned with e-commerce transactions or health information, in many cases make use of a trustmark program to demonstrate that the content of their site meets a common set of standards. This set of standards is usually set out in a written code of conduct.[54] One example in this respect the TRUSTe trustmark, an on-line, branded seal, which is displayed by members of the TRUSTe's licensing program. Only those web sites that meet the privacy principles established by the On-line Privacy Alliance (OPA) and agree to comply with TRUSTe oversight and dispute resolution are allowed to display the TRUSTe seal. Members of the TRUSTe's licensing program are obliged to post a privacy policy on their web site, which discloses on-line information gathering and dissemination practices. In case of a privacy violation, they are contractually liable to an examination of their privacy practices.[55] A similar example that can be mentioned here is the introduction of hallmarks for secure e-commerce in specific geographical areas or sectors, like TrustUK.[56] However, the application of this self-regulatory instrument might lead to the development of trade barriers, as a higher level of consumer protection may be requested from specific companies.

---

representatives of all parties involved, including the business community and scientific research organizations, government agencies, and consumer organizations.

[52] The Centre for Trade Facilitation and Electronic Business of the United Nations (UN/CEFACT) adopted the Recommendation regarding 'E-commerce self-regulatory instruments' which included the Model Code of Conduct for Electronic Commerce (Draft version 3.0) as an example. See < http://www.unece.org/cefact/recommendations/rec32/rec32_ecetrd277.pdf >.

[53] See *supra* n. 32, at , p. 123.

[54] Bennett & Raab 2003.

[55] Ibid.

[56] <www.trustuk.org.uk>, last visited October 2004.

The Pan European Games Information rating system (PEGI) for video games and other media content can be mentioned as an example of self-regulation regarding content assessment. Implemented by the Interactive Software Federation of Europe (ISFE) in 2003 and with sixteen European countries participating since March 2004, the PEGI content rating system is a collaborative effort of national self-regulatory organizations and industry. The content rating system embodies five age categories (3, 7, 12, 16, and 18) and six content descriptors with warnings respectively regarding discrimination, drugs, fear, bad language, sex, or violence.

An example of what many authors perceive as a pure form of self-regulation are domain-name dispute resolutions mechanisms, such as the Uniform Domain Name Dispute Resolution Policy (UDRP) adopted by the Internet Corporation for Assigned Names and Numbers (ICANN) in 1999. The UDRP is based on recommendations made by WIPO. If a trademark holder thinks that a domain name registration infringes on his trademark, he may initiate proceedings under this Policy. The UDRP permits complainants to file a case with a resolution service provider, i.e., the WIPO Arbitration and Mediation Center, specifying the domain name in question, the respondent or holder of the domain name, the registrar with whom the domain name was registered, and the grounds for the complaint. Such grounds include the reason why a domain name is identical or similar to a trademark to which the complainant has rights; why the respondent should be considered as having no rights or legitimate interests in respect of the domain name that is the subject of the complaint; and why the domain name should be considered as having been registered and used in bad faith.[57] Respondents are given the opportunity to defend themselves against the complaint. Moreover, the WIPO Arbitration and Mediation Center appoints a panelist who decides on the potential transfer of the domain or domains.[58]

#### 5.3.4.2 *Standards*

Standards are an example of self-regulatory arrangements which not only imply the availability of a common code but also a conformity assessment procedure. In 1996, the Model Code for the Protection of Personal Information was approved as a National Standard of Canada by the Standards Council of Canada.[59] This standard is based on ten principles, which organizations are advised to adopt in their entirety. Any public or private organization that processes personal data may adopt this voluntary instrument. Once adopted, however, the standard implies that certain obligations must be followed through in the event of organizational claims.

Other examples of standards or attempts towards standardization are negotiations towards a certifiable management standard for data protection through the

---

[57] <http://arbiter.wipo.int/center/faq/domains.html#16>, last visited October 2004.
[58] <http://arbiter.wipo.int/domains/>, last visited October 2004.
[59] See *supra* n. 32, at p. 127.

International Standardization Organization (ISO), later followed by similar attempts via the Comité Européen de Normalisation (CEN).[60]

#### 5.3.4.3 *Netiquette*

Netiquette is considered to be the general network etiquette or etiquette of Internet users. Etiquette means, 'forms required by good manners or prescribed by authority to be needed in social or official life.' Netiquette is thus a set of basic rules for Internet users on how to behave properly on-line. Netiquette embodies the following set of guidelines for general behavior in various on-line environments:[61]

> 'Rule 1: Remember the Human: Do unto others as you'd have others do unto you.
> Rule 2: Adhere to the same standards of behavior on-line that you follow in real life: Breaking the law is bad netiquette.
> Rule 3: Know where you are in cyberspace: What's perfectly acceptable in one area may be dreadfully rude in another.
> Rule 4: Respect other people's time and bandwidth: When you send email or post to a discussion group, you're taking up other people's time (or hoping to). It's your responsibility to ensure that the time they spend reading your posting isn't wasted.
> Rule 5: Make yourself look good on-line: You will be judged by the quality of your writing. For most people who choose to communicate on-line, this is an advantage; if they didn't enjoy using the written word, they wouldn't be there. So spelling and grammar do count.
> Rule 6: Share expert knowledge: The Internet was founded and grew because scientists wanted to share information. Don't be afraid to share what you know.
> Rule 7: Help keep flame wars under control: Netiquette does forbid the perpetuation of flame wars. Flame wars are series of angry letters, most of them from two or three people directed toward each other, that can dominate the tone and destroy the camaraderie of a discussion group.
> Rule 8: Respect other people's privacy: Of course, you'd never dream of going through your colleagues' desk drawers. So naturally you wouldn't read their email either.
> Rule 9: Don't abuse your power: Knowing more than others, or having more power than they do, does not give you the right to take advantage of them. For example, sysadmins should never read private email.
> Rule 10: Be forgiving of other people's mistakes: Everyone was a network newbie once. So when someone makes a mistake – whether it's a spelling error or a spelling flame, a stupid question or an unnecessarily long answer – be kind about it. If it's a minor error, you may not need to say anything. Even if you feel strongly about it, think twice before reacting. Having good manners yourself doesn't give you license to correct everyone else.'

---

[60] As described by Bennett & Raab 2003.

[61] These guidelines for on-line behavior were excerpted from Virginia Shea, Netiquette, Albion Books, 1994.

These Netiquette guidelines do not take into account all kinds of problems resulting from deviant on-line behavior, but provide basic principles that can be used to solve dilemmas in deciding upon on-line behavior. Netiquette rules can be further adjusted by any organization for their own users, clients, employees, etc.

### 5 3.4.4 *Public watchdogs and hotlines*

Internet does not only offer 'good' or lawful information and activities to its users, but also comprises illegal and harmful information, materials, or behavior. Examples in this respect are child pornography, discriminatory information, or illegal offers of medication. As traditional law enforcement turned out to be a complex matter for the deterritorialized, border-less Internet, self-regulatory instruments like public watchdogs and hotlines have been created as alternative solutions for this gap.

A public watchdog organization internationally considered as a model organization is the Internet Watch Foundation (IWF). In 1996 as public concern about illegal and offensive material on the Internet was increasing, the UK Department of Trade and Industry (DTI) facilitated discussions between ISPs, the London Metropolitan Police, the UK Home Office and an organization called the Safety Net Foundation. These discussions resulted in the 'R3 Safety Net Agreement', with R3 referring to the triple approach of Rating, Reporting, and Responsibility. This agreement resulted in the establishment of the IWF as the responsible body for implementing this voluntarily established arrangement for monitoring and tackling illegal and offensive content on the Internet. The IWF has three main roles:

1. It operates a hotline where UK Internet users can report on-line material which they believe might be illegal. If the IWF supports this view, it passes on the relevant information, either to the Metropolitan Police (if the alleged offence has been committed in the UK) or to the National Criminal Intelligence Agency (if the alleged offence has been committed in another country);
2. Together with other relevant organizations, it promotes voluntary systems for the rating of Internet content and the use of filtering techniques to enable parents, teachers and others responsible for children to prevent children in their care from gaining access to illegal, offensive, or inappropriate materials;
3. In partnership with many other organizations, the IWF has an education and awareness role so that some of the problems of Internet use, particularly the risks to children, and the mechanisms for dealing with these problems will become better known and understood.

The global nature of the Internet as well as the fact that over 90 per cent of all pornographic material accessed by UK Internet users is hosted outside the UK bring in the need for an international focus of the IWF in its activities. Consequently, the IWF strongly supports the Internet Hotline Providers in Europe (INHOPE) association as well as the Internet Content Rating for Europe (INCORE) organization.

In the Netherlands, ISPs united in the Dutch Foundation for Internet Providers (NLIP) developed a policy to be able to act against available materials on-line that under Dutch law are illegal. Part of this policy is the joint establishment by ISPs and consumers of hotlines [*meldpunten*] against child pornography, discrimination, and illegal content where on-line illegal materials can be reported. After notification, the hotline or ISP will test the reported content against existing Dutch laws and rules. The Dutch hotlines are only able to act in accordance with Dutch national legislation, and therefore only against offenders or information suppliers residing in the Netherlands. Notifications concerning offenders or information suppliers residing in other countries are reported to foreign watchdogs wherever possible.

Generally, the observation can be made that ISPs have been under pressure regularly to become more involved in monitoring, evaluating, rating, and removing Internet content. So far, they have resisted most involvement, arguing that they are mere conduits of information and that additional regulatory functions would burden them with unreasonable costs.[62] However, with policy and financial support of the European Commission and national governments, ISPs have evolved towards a new model of self-regulation in the form of Notice and Take Down (NTD) procedures operated through telephone hotlines. In twelve European countries, there are sixteen hotline services, at present, with the following general characteristics.[63]

- They operate primarily to facilitate removal and law enforcement in dealing with content that is clearly illegal in any medium. What is illegal, however, varies from state to state (for example, varying interpretations of hate speech, varying legal treatments of racist speech). The majority of complaints and actions relates to child pornography. Other forms of content taken down through hotlines include copyright infringement and defamatory and racist material.
- Complaints are roughly dealt with according to the following procedure: ascertaining if content is illegal; passing on relevant information to law enforcement; informing the ISP that the material is hosted on its servers, and take down of that content by the ISP.
- ISP hotline organizations have become involved in other forms of self-regulatory activities as well, for example, in the promotion of filtering, awareness, and rating technologies. Moreover, they have been proactive in raising awareness of other child-protection issues on the Internet, particularly with regard to chat-room danger and privacy.

#### 5.3.4.5 *Technology as self-regulation*

Not only organizational solutions exist to arrive at self-regulatory arrangements, the technology itself also offers opportunities for self-regulation.

---

[62] <www.selfregulation.info>, last visited October 2004.

[63] See *supra* n. 47.

As an example, technological mechanisms exist that can anonymize information which is usually associated with certain individuals, such as anonymous remailers for electronic mail or anonymous browsers for Internet surfing. These Privacy Enhancing Technologies (PETs) can be found in other forms as well. Besides instruments for anonymity and pseudonymity, as mentioned, Bennett and Raab distinguish the following types of instruments that provide individual empowerment regarding on-line privacy protection:[64] encryption instruments (for example, e-mail encryption programs); filtering instruments (for example, filtering software to block and delete cookies); and Privacy Management Protocols (for example, privacy preference protocols like the Platform for Privacy Preferences (P3P) initiative, set-up by the World Wide Web Consortium).

Another technological development that provides a new form of self-regulation are Digital Rights Management Systems. These systems can automate permission as well as payment for the use of copyright-protected works. Secure viewers can also be used to assure that an owner's choice of restrictions will be self-executed.

## 5.4 When Should It Apply?

The self-regulatory schemes that have been established thus far – section 5.3 offers only a small selection of initiatives – appear helpful mechanisms in dealing with the variety of regulatory gaps on the Internet or complementing and reinforcing existing legal frameworks. In itself, the development of self-regulatory initiatives as well as their diversity appears welcome. However, the question arises to what extent and under what circumstances and conditions they may be helpful. While codes of conduct, seals, hotlines, trustmarks, and other instruments potentially add value to tackling the numerous problems that users face in the on-line environment, these instruments may also have their drawbacks. There is, for example, concern that there is no set of benchmarks by which parties can judge the relative merits of the instruments. Also, what self-regulatory initiatives can genuinely be trusted? Are the criteria for granting seals and trustmarks transparent, neutral and objective? What about the monitoring and enforcement of self-established rules? And what are the cross-border implications, given that the majority of the initiatives merely cover the situation in a specific country? So, is the rapidly multiplying variety in scope, geographical coverage, participation and oversight of the hundreds of ICT-related self-regulatory initiatives in itself a welcome development?

In the remaining part of this chapter we will aim to develop criteria to determine when self-regulation should – or should not – be considered and try to define in how and to what extent self-regulation should indeed be a starting point for ICT regulation. First, we will indicate some relevant criteria, starting with several lists

---

[64] See *supra* n. 32, at pp. 148-153.

of criteria suggested by policy documents. We will subsequently cluster these into seven broad criteria.

### 5.4.1 Criteria in policy documents

According to the Dutch government, self-regulation is the starting point (see 5.2.2.2), but not at all costs:

> 'Self-regulation as an alternative to government regulation is not suitable if fundamental norms and values of the democratic rule of law are at stake. In the case of the electronic highway, this holds especially with respect to protecting classical human rights of citizens and preventing and investigating infringements of the rule of law and state security. In these cases, agreements between parties cannot suffice and legislation will be necessary.'

Moreover, in order to be acceptable as an alternative to government regulation, self-regulation has to meet several elementary conditions:

- the relevant groups must be well-organized;
- relevant social interests must be equally protected;
- all parties must be sufficiently bound to the rules;
- enforcement of the rules must be sufficiently guaranteed.

In the long run, however, government regulation might become the starting point again.

This may be the case if:

- developments lead to replacement, i.e. when people can no longer do things off-line but can only perform them on-line. The government should then create guarantees for accessibility;
- technological turbulence decreases and stability is achieved. Then, to promote legal certainty, perhaps codification of norms established by self-regulation could take place.[65]

In the 2001 White Paper on European Governance, the European Commission also lists various criteria for private regulation in the form of co-regulation: 'Co-regulation implies that a framework of overall objectives, basic rights, enforcement and appeal mechanisms, and conditions for monitoring compliance is set in the legislation.' When can co-regulation be considered?

---

[65] See *supra* n. 17, at pp. 181-182.

> 'It should only be used where it clearly adds value and serves the general interest. It is only suited to cases where fundamental rights or major political choices are not called into question. It should not be used in situations where rules need to apply in a uniform way in every Member State. Equally, the organizations participating must be representative, accountable and capable of following open procedures in formulating and applying agreed rules. This will be a key factor in deciding the added value of a co-regulatory approach in a given case.
> Additionally, the resulting co-operation must be compatible with European competition rules and the rules agreed must be sufficiently visible so that people are aware of the rules that apply and the rights they enjoy. Where co-regulation fails to deliver the desired results or where certain private actors do not commit to the agreed rules, it will always remain possible for public authorities to intervene by establishing the specific rules needed.'[66]

In the US Department of Commerce indicated criteria for regulating privacy in e-commerce:

> 'In order to empower consumers to have control of their own personal information, the US government is encouraging the private sector to establish codes of conduct and self-regulation. To be meaningful, the government believes that self-regulation must do more than articulate broad policies or guidelines. Effective self-regulation involves substantive rules, as well as the means to ensure that consumers know the rules, that companies comply with them, and that consumers have appropriate recourse when there is noncompliance.'[67]

Some other aspects emerge in the US FTC's recommendations on on-line profiling, where it concluded that legislation seems necessary to enforce industry guidelines.[68]

> 'As the Commission has previously recognized, self-regulation is an important and powerful mechanism for protecting consumers, and the NAI principles present a solid self-regulatory scheme. Moreover, NAI members have agreed to begin to put their principles into effect immediately while Congress considers the Commissions recommendations concerning on-line profiling.
> Nonetheless, backstop legislation addressing on-line profiling is still required to fully ensure that consumers' privacy is protected on-line. For while NAI's current membership constitutes over 90% of the network advertising industry in terms of revenue and ads served, only legislation can compel the remaining 10% of the industry to comply with fair information practice principles. Self-regulation cannot address recalcitrant and bad actors, new entrants to the market, and dropouts from the self-regulatory pro-

---

[66] See *supra* n. 4, at p. 21.

[67] Department of Commerce, *The Emerging Digital Economy*, April 1998, <http://www.technology.gov/digeconomy/emerging.htm>.

[68] Federal Trade Commission, *On-line Profiling: A Report to Congress. Part 2: Recommendations*. July 2000. On the Internet: <http://www.ftc.gov/os/2000/07/on-lineprofiling.htm#III.%20RECOMMENDATIONS>.

gram. In addition, there are unavoidable gaps in the network advertising companies ability to require host Websites to post notices about profiling, namely Web sites that do not directly contract with the network advertisers; only legislation can guarantee that notice and choice are always provided in the place and at the time consumers need them.'

The Australian Taskforce on Industry Self-Regulation referred to a general guide as to whether self-regulation is appropriate: the Commonwealth Office of Regulation Review's Regulatory Impact Statement checklist. This checklist states that:

'self-regulation should be considered where:
- there is no strong public interest concern, in particular, no major public health and safety concern;
- the problem is a low risk event, of low impact/significance, in other words the consequences of self-regulation failing to resolve a specific problem are small; and
- the problem can be fixed by the market itself, in other words there is an incentive for individuals and groups to develop and comply with self-regulatory arrangements (for example, for industry survival, or to gain a market advantage).

In addition, for self-regulatory industry schemes, the checklist determines success factors to include:
- presence of a viable industry association;
- adequate coverage of the industry by the industry association;
- cohesive industry with like minded/motivated participants committed to achieving the goals;
- voluntary participation – effective sanctions and incentives can be applied, with low scope for the benefits being shared with non-participants; and
- cost advantages from tailor-made solutions and less formal mechanisms such as access to quick complaints handling and redress mechanisms.'[69]

This checklist is analyzed and elaborated in the report, with attention paid to, among other issues, adequate coverage, clarity, consumer and industry awareness, transparency, dispute procedures and sanctions for non-compliance, monitoring, reviewing, accountability, and costs. There can be no one-size-fits-all guidelines for self-regulation, but the 'appropriate form of self-regulation will depend on what is trying to be achieved, which will vary depending on the industry.'[70]

The World Summit on the Information Society's Declaration of Principles outlined key principles for building an inclusive information society.[71] One of these key

---

[69] <http://www.selfregulation.gov.au/publications/TaskForceOnIndustrySelf-Regulation/FinalReport/isr_part2-05.asp>.

[70] <http://www.selfregulation.gov.au/publications/TaskForceOnIndustrySelf-Regulation/FinalReport/isr_part2-06.asp>.

[71] World Summit on the Information Society, *Declaration of Principles*, Document WSIS-03/GENEVA/DOC/4-E (12 December 2003), available at <http://www.itu.int/wsis/documents/>, p. 3.

principles is to create an enabling environment, which gives an indication of when governments should intervene:

> 'The rule of law, accompanied by a supportive, transparent, pro-competitive, technologically neutral and predictable policy and regulatory framework reflecting national realities, is essential for building a people-centered Information Society. Governments should intervene, as appropriate, to correct market failures, to maintain fair competition, to attract investment, to enhance the development of the ICT infrastructure and applications, to maximize economic and social benefits, and to serve national priorities.'

### 5.4.2 **Main criteria**

Various policy papers have thus listed sets of criteria for situations in which self-regulation can be considered and when government intervention is called for. These can be summarized as follows.

*1. Fairness*

A broadly shared view is that regulatory rules should be fair. That is, social interests should be protected, particularly those of weaker parties who may not have been able to participate in the regulatory process or whose interests might be crushed under the weight of industry interests.[72] Equality, non-discrimination, fundamental rights and fair competition should be safeguarded if 'replacement' occurs, that is, if people can no longer fall back on traditional means and ways of doing things, situations should be avoid in which certain groups in society fall behind, for instance, because they lack relevant ICT skills of the new communications media.

Fairness is one of the prime indicators for government involvement. If fundamental rights are at stake or if certain groups threaten to be discriminated, self-regulation is not an adequate instrument. Safeguarding all relevant interests, particularly those of weaker parties cannot be left to private actors.

*2. Inclusiveness*

A second criterion is the inclusiveness of the self-regulatory process: who participates in drafting rules and do these participants constitute a sufficiently representative sample of the relevant actors? For self-regulation to work, the stakeholders should be well organized in order to ensure that the people participating in the process know the needs and desires of their colleagues and the people they represent.

Although this criterion is related to the first, in that the self-regulatory process works better if interest groups representing weaker parties participate, it is a sepa-

---

[72] Cf., the Law Council of Australia's comment that 'a minimum condition for successful self-regulation is the provision of industry funded independent consumer representatives, so that the various uneven elements of the consumers/producer relationship can be remedied', <http://www.self regulation.gov.au/publications/TaskForceOnIndustrySelf-Regulation/FinalReport/isr_part2-06.asp>.

rate issue. 'Fairness' looks at subject-matter and results, indicating that where complex balancing issues involving fundamental rights are at stake, self-regulation usually will not work and the government should keep a close eye on developments. 'Inclusiveness' is a criterion for those issues that, in principle, lend themselves well to self-regulation; it stresses that the effectiveness of self-regulatory rules will depend on the representativeness of the actors that take part in drafting the rules.

*3. Compliance*

Perhaps most often cited as a primary concern with self-regulation is the issue of compliance. To what extent and with what instruments can organizations that self-declare their standards of communication or behavior be held accountable if their initiatives fail to live up to the expectations of consumers, citizens, or other parties in the on-line world? What, for example, to do with businesses that apply privacy seals, but fail to provide the expected level of care? A crucial difference with government regulation is that, with self-regulatory rules, there is not a natural mechanism to ensure compliance. In principle, self-regulatory mechanisms do not establish law in the meaning of legal rules that are binding on all citizens in a certain country (for the very reason that self-regulatory mechanisms are not created by democratic means such as control by an elected parliament). Thus, a key disadvantage of self-regulatory schemes is their lack of adequate enforcement.[73] Hence, considerable attention must be given to enforcement mechanisms. Since the mere creating of rules does not make the self-regulating parties accountable for complying with the rules, various instruments may be considered to enhance accountability, such as monitoring committees and procedures, and complaint-handling and dispute resolution mechanisms.

In fact, a closer look at self-regulation initiatives reveals that various enforcement scenarios appear in practice. First, organizations may decide to enforce the self-declared rules themselves. Many responsible organizations indeed try to ensure the adherence to the norms they have set, either by sanctions (for example, by ejection from membership or by denying further use of a trustmark), by means of labeling, and by rating mechanisms. However, the characteristics of the on-line world make it difficult to effectively sanction parties who fail to respect these norms. Ensuring that the initiative passes from letter to action appears, in particular, to be difficult in light of the borderless environment in the on-line world. Also, since self-regulatory sources are often located only in a certain territory or that the initiatives are often limited to a group of actors who share a certain attitude towards professional behavior, the overall effect of self-regulatory initiatives may be questioned. For if an organization lacks the means, power, and authority to enforce its norms, then their value remains symbolic. Thus, a convincing case for self-regulation can only be made if the relevant parties to the self-imposed rules or standards formulate organizational compliance measures with inherently binding provisions,

[73] See on this in detail: Prins, Schellekens, 2004.

for example, in operational policies. But as the FTC has noted, unwilling actors must also be taken into account: 'Only legislation can compel the remaining 10% of the industry to comply with fair information practice principles. Self-regulation cannot address recalcitrant and bad actors, new entrants to the market, and drop-outs from the self-regulatory program.' That is to say, self-regulation works well with willing actors, but as long as a certain part of the market has an interest in not complying, self-regulation alone cannot do the trick. In the end, the effectiveness of self-regulation largely depends on the internal discipline of the organization or group of actors. Thus far, very little research has been done to measure the exact commitment of the partners in a self-regulatory scheme.

In a way, the issue of compliance mirrors the criterion of inclusiveness: the more involved all stakeholders are in drafting self-regulatory regimes, the better incentive they will have to comply with the rules. In other words, in domains and processes in which a high level of involvement of all relevant actors is ensured, perhaps less attention need be given to enforcement mechanisms. The reverse is also true: the less actors participate in self-regulation, the more compliance becomes an issue. In those cases, if insufficient legal instruments are or can be created for compliance, regulation is more a matter for government than for private parties.

*4. Transparency*

Almost equally frequently mentioned as a concern with respect to self-regulation is the transparency of the process of drafting rules or of the resulting rules themselves. Contrary to (the theory of) democratic rule-making, self-regulation may be an obscure and behind-the-scene process. If the people affected by self-regulation are not made aware of the process, they cannot try and influence it to their benefit (compare also the criterion of fairness); and if the resulting rules are invisible or untransparent, they cannot complain if they are adversely affected.

Transparency is related to the effectiveness of the regulation: self-regulatory rules that are opaque (for example, seals or trustmarks with obscure criteria) will be less trusted and hence not readily followed. In that sense, transparency is also related to compliance: since self-regulation is usually done by a selection of private parties, the non-participating actors will not be willing to comply, unless the process and rules are sufficiently transparent for them to adopt the rules voluntarily.

*5. Legal certainty*

Comparable to transparency is the issue of legal certainty: are rules sufficiently clear, unequivocal, and consistent to provide the legal certainty needed by actors in a certain field? As with legislation, this is an important issue. However, it is not easy to say whether legal certainty in general is an argument for or against self-regulation. In some cases, self-regulation is better suited to provide legal certainty, for instance, if the field is rapidly changing and flexibility in updating rules is called for. Moreover, self-regulation might be seen as a better instrument for very detailed rules, while legislation is more suited to general and more abstract rules. However,

this argument is not backed up by legislative practice: large areas of the law are extremely detailed. Indeed, sometimes the law does need to be detailed in order to provide the right level of legal certainty, while self-regulation may equally well lose itself in vague rules that leave much room for interpretation. Hence, it should be considered whether the subject-matter and the actors involved in self-regulation are sufficiently able to draft clear and precise rules, or whether this particular subject-matter is more suited for government regulation to provide adequate legal certainty.

*6. Context*

This brings us to the more general criterion of context. As the Australian taskforce noted, much depends on what self-regulation tries to achieve, and this varies, depending on the industry and subject-matter. It also depends on the technology at issue, as the Dutch criterion of technological turbulence shows.

Also relevant is the international context: is the subject something which can be fairly well regulated in a national context? Is it an issue with a large variety of initiatives around the world? Is it something that calls for harmonization? Note that, like legal certainty, the international context is not necessarily something that favors self-regulation: although it might be said that, at an international level, self-regulation is easier to achieve than government regulation (compare chapter 6), it is not obvious that a multitude of private parties around the world can achieve harmonized rules better than governments. This, again, also depends on the subject-matter, the industries, and the technologies involved.

Another dimension of the context is politics: self-regulation is more suited to 'neutral' issues: issues that call for answers (what electronic signatures have sufficient legal validity?) rather than policy choices (should spam be allowed or restricted?).[74] If major political choices are at stake democratically elected governments should make them, not private parties.[75]

*7. Efficiency*

Last and perhaps least on a theoretical level, but foremost on a practical level, is the issue of efficiency. Government regulation is often regarded as cumbersome, time-consuming, and costly, while self-regulation is seen as swift, meager, and cheap. Moreover, self-regulation is more flexible and therefore better suited for regular updating with developments. This does not only relate to the process of regulation: self-regulation may also impose lower compliance costs on businesses because they themselves can better tailor the rules to their situation.

---

[74] In the terminology of our earlier report on internationalization: 'answering issues' are more suited to self-regulation than 'steering issues'. See Koops, et al., 2000, p. 173.

[75] Compare the Australian Taskforce's principle 34: Government involvement in self-regulation is justified when there is a public policy objective that would otherwise call for a regulatory response', <http://www.selfregulation.gov.au/publications/TaskForceOnIndustrySelf-Regulation/FinalReport/isr_part2-07.asp>.

This is not to say that self-regulation should therefore be the starting point, but it does mean that if other criteria do not indicate a clear preference for government regulation, self-regulation is the natural first choice. In other words, efficiency is a criterion that becomes prominent if the other criteria give insufficient guidance in choosing between self-regulation and government regulation.

## 5.5 How Can It be Applied?

Taking the criteria listed above into consideration, it appears that there will seldom be a preference for pure self-regulation. If the subject-matter is not contentious, if the stakeholders participate in a transparent process with sufficient respect for all interests at stake, with compliance ensured by effective self-enforcement and a 100 per cent involvement of all market parties, and with awareness-raising mechanisms for consumers, then pure self-regulation is a good starting point indeed. But this will rarely be the case.

Nearly all policy documents as well as the literature stress that there is also a role for the government. Just what this role is, is less clear – there is a large variety of options and types of government intervention to chose from. The criteria outlined above may give a clue to the right level of government action.

In this section, we will indicate various roles for the government and mechanisms for enhancing the efficacy of self-regulation, which all can be deemed some type of co-regulation. We distinguish between legislative action, procedural action, and other facilitating action.

### *1. Legislative action*

#### *1.1 Codification*

A straightforward way of enhancing the efficacy of self-regulation is to codify in law the norms that have been created by self-regulation. It is one of the traditional types of co-regulation in the form of stipulated self-regulation (see section 5.3.2). This has been suggested by the Australian taskforce as one of their conclusions: '36. Government can assist in integrating schemes into the regulatory framework.'[76] It is also what the Dutch government suggested as an option when turbulent times have calmed down and self-regulatory norms have crystallized, in order to enhance legal certainty.[77]

Codifying self-regulatory rules does not only enhance legal certainty, but it also strengthens compliance, since legal norms are usually easier to enforce than self-regulatory norms. Of course, it should only be considered for self-regulation that is additional to and consistent with existing legal norms, and only if the subject-mat-

[76] <http://www.selfregulation.gov.au/publications/TaskForceOnIndustrySelf-Regulation/FinalReport/isr_part2-07.asp>.

[77] See *supra* n. 17, at p. 182.

ter is not contentious and the norms are widely shared by the stakeholders. If the self-regulation was flawed in some sense, for instance, if interests of vulnerable groups were insufficiently taken into account, the government should consider new or other regulation rather than codification.

*1.2 Backstop legislation*

In many cases, self-regulation will not by itself be completely satisfactory where, for instance, the criteria of fairness or inclusiveness are concerned. In such cases, 'backstop' legislation can be considered, as the FTC suggested: 'Backstop legislation addressing on-line profiling is still required to fully ensure that consumers privacy is protected on-line.'

Such backstop legislation can take various forms. It can be enacted pro-actively, as an incentive for market parties to develop self-regulation. Such legislation can offer incentives, such as providing legal certainty for parties that comply with standards to be developed by industry. Examples of this are the Directive on digital signatures (providing evidential value for signature schemes compliant with the Annexes criteria) and the 'safe harbor' that the US CALEA Act offers telecom carriers who comply with publicly available technical requirements or standards adopted by an industry association or standard-setting organization for interceptability of telecommunications (47 USC § 1006). Alternatively, the law may use a stick rather than a carrot and threaten with legislation if adequate self-regulation is not forthcoming. An example of this is the DRM provision in the Copyright Harmonization Directive:

> 'In the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law'.

Threatening with legislation if self-regulation does not meet the criteria determined by government, is one of the instruments mentioned by the Dutch government (see section 5.4.1).[78] Apart from pro-active legislation, backstop laws may also be enacted ex post, for instance, to push recalcitrant actors into complying with self-regulatory schemes developed by others. It should also be considered as soon as self-regulation appears not to work. As one of the conclusions of the Australian taskforce stated: 'The degree of government involvement will depend on the significance of the market failure or social policy objective being addressed and the consequences of self-regulation proving ineffective.'[79]

---

[78] Ibid., at p. 181.

[79] <http://www.selfregulation.gov.au/publications/TaskForceOnIndustrySelf-Regulation/FinalReport/isr_part2-07.asp>, conclusion 38.

*1.3 General framework legislation*

Rather than enacting pro-active or ex post incentives or retaliatory legislation, the government can also establish a general framework, for instance, with minimum standards or conditions, in which self-regulation can subsequently take place. 'In this hybrid form of self-regulation, the legislator takes the initiative and determines the frameworks in which the self-regulation has to take place. For example: only the further technical detailing is left to market parties and private normalization bodies. As far as such stipulated self-regulation constitutes further detailing of government responsibilities, a number of formal and procedural requirements will hold. These do not differ in the electronic environment from those in the traditional environment.'[80]

The framework may be more basic than to only leave room for 'technical detailing'. The framework could also consist of some basic norms that have to be safeguarded, while leaving open other issues and the way in which those norms will be satisfied. This could be a viable option with respect to codes of conduct, where there is currently a highly diverse landscape of – often conflicting – standards for conduct and on-line behavior. Illustrative is the variety in substantive rules included in the codes of conduct of the Web trader initiative established by the consumer associations in different European countries. The present situation made Endeshaw argue that: '[t]he functional diversity and overlap, on the one hand, and the conflicting standards among trustmarks, on the other hand, prompt a coherent solution.'[81] A possible solution is the e-Confidence program of the European Commission, which examines the possibility for drawing up common guidelines for e-commerce codes of conduct; these guidelines could be used by bodies responsible for monitoring and approving codes of conduct. Thus far, no Recommendation has been published; a second draft of the framework principles was produced by a group of business and consumer stakeholders and published for comment in early 2001.[82] A related initiative (also part of the EU e-Confidence project) is that of BEUC and UNICE to establish a set of requirements for trustmark schemes, the European Trustmark Requirements.[83]

Nevertheless, it could be questioned to what extent standardization and certification of trustmarks, codes of conduct, seals, and other self-regulatory initiatives should be a goal in itself. It could be argued that a diversity in schemes and their content is in itself welcome, because it encourages competition between standards and thus, over time, may enhance the quality and level of the standards. It would

---

[80] See *supra* n. 17, at p. 184.

[81] Endeshaw 2001, p. 225.

[82] The texts of the first and second drafts as well as the comments made by various organizations are available at <http://econfidence.jrc.it>. The second draft of principles contains ten general principles for generic codes of practice for the sale of goods and services to consumers on the Internet: Fairness and equity, Added value, Transparency, Openness and non-discrimination, Global dimension, Social responsibility, Compliance, Complaint handling and dispute resolution, Security, and Data protection.

[83] Also available at <http://econfidence.jrc.it>.

also provide consumers and businesses with a wider choice. What is more, setting certain standards for self-regulatory initiatives may not offer a definitive solution to the present landscape of highly different substantive rules. Even with a general framework of basic principles, disparity in national laws regarding the status and enforcement of self-regulatory initiatives will continue to affect the end result of the initiative. Individual countries may also try and compete on the use or non-use enforcement mechanisms. For example, despite the availability of guidelines, one country might decide to close the door to foreign initiatives (such as a foreign trustmark) and provide its own businesses with advantages. In its reaction to the second draft of the European Union Principles on E-Commerce Codes of Conduct, the US Federal Trade Commission expressed a view in line with this point: 'We have concerns that approval of codes could have a discriminatory effect on US businesses and could therefore deter the growth of an international electronic marketplace.'[84]

Perhaps needless to stress, framework legislation is always appropriate when fundamental rights are at stake (see the fairness criterion in section 5.4.2). As the final conclusions of the OECD Forum on Electronic Commerce stressed, it is the responsibility of national governments 'notably to protect vulnerable groups'.[85] This protection can only be achieved by legislation that sets basic standards for protection of weak parties and for fundamental rights.

*1.4 Procedural legislation*

Similar to creating framework legislation with basic substantive principles, governments could also enact legislation that sets procedural requirements for self-regulation. An example is the drafting of sectoral codes of conduct for data protection. The Directive on the protection of personal data encourages the drafting of codes of conduct for data protection,[86] and organizations can request the Data Protection Authority (DPA) to declare that, given the particular features of the sector or sectors of society in which these organizations operate, the rules contained in their code properly implement the Personal Data Protection Act or other legal provisions on the processing of personal data. However, the DPA may only consider requests

[84] Comments on the Second Draft Principles for E-Commerce Codes of Conduct made by the US Federal Trade Commission Staff, 18 April 2001, available at <http://econfidence.jrc.it>.

[85] OECD Forum on Electronic Commerce, *Report on the Forum*, Paris, 12-13 October 1999, p. 13. Likewise the 1997 Ministerial Conference in Bonn, in which the EU ministers concluded that the main role for the legislator is to safeguard fundamental norms and values in an electronic environment. European Commission, *Ministerial Declaration*, Ministerial Conference, Bonn, 6-8 July 1997, <http://europa.eu.int/ISPO/bonn/Min_declaration/i_finalen.html>.

[86] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Recital 61. In practice, the benefit of such a 'conformity declaration' lies in the added certainty for those who work with personal data that their handling of personal data is lawful if and when they align their behavior with the code of conduct. Codes of conduct are in effect so complete in their coverage of subjects that those working with personal data in the pertinent sector need not have recourse to other legal sources.

where, in its opinion, the organizations that request recognition are sufficiently representative, and the sector or sectors concerned should be adequately defined in the code of conduct. Moreover, if the code includes a dispute resolution mechanism, a declaration of conformity can only be considered if sufficient guarantees for independence are given.[87]

*1.5 Liability*

Not purely a legislative action, but a traditional legal instrument nonetheless, is liability. The majority of the current self-regulatory initiatives aim at making promises to the outside world: they publicly claim – implicitly or explicitly – that users can depend on a certain level of privacy or consumer protection, a minimum standard of the quality and credibility of the on-line services, etc. This raises expectations with the general public and specific consumers. As a result, the presentation tends to enhance the standard by which the conduct of those applying the initiative is measured. The fact that the applicable norms, definitions, and responsibilities have been made explicit makes it, in general, easier to successfully win a liability case. In other words, when the claimed or expected results of the self-imposed initiative turn out to be not as expected or do not materialize at all, the self-regulatory parties may be held liable for any resulting damage.[88]

Of course, this will only be the case if a contractual relationship exists between the organization that initiated the self-regulatory scheme (for example, a code of conduct established by the representative body of ISPs) and a member of that organization (for example, an individual ISP). For example, an ISP may thus be accountable to the organization for any operation not in accordance with the code of conduct. On its part, the organization may be held liable if it did not exercise due care and skill in accepting new members, monitor its members' activities and take appropriate steps to remedy unwanted operations of members. In the absence of adequate monitoring and enforcement, the success of the code of conduct may be comprised and thus become less 'trustworthy', which could have negative consequences for the other members of the organization.

Contractual liability may also play a role in enforcing self-regulatory mechanisms in the relation between electronic businesses and consumers. For example, when a trustmark or seal is put up on the web site of an on-line shop, an aggrieved consumer who was misled may seek to pursue a contractual liability action.

However, this option would only seem available when the relationship between the on-line shop and the consumer is entirely contractual and the 'promises' behind the trustmark are somehow integrated into the contract. In all other situations, a contractual liability claim will not find any legal support. In certain situations, liability under tort law may then provide an alternative for enforcement. However, whether a consumer's claim succeeds will depend on many circumstances, such as

[87] See, for example, Art. 25 of the Dutch Personal Data Protection Act.
[88] Prins & Schellekens 2004.

the nature and explicitness of the 'promises', the additional claims as to the role the trustmark plays, the type of consumer.

It is in the absence of a contractual relationship that the lack of enforcement tools becomes most evident. As mentioned, self-regulatory mechanisms do not establish law in the meaning of legal rules that are binding on all citizens in a certain country. Thus, a third party that is not a participant in the self-regulatory scheme is, in principle, not obliged to follow any suggestions the body might make. In fact, it may do nothing. This is a rather unsatisfactory situation, given the numerous self-regulatory initiatives that have appeared in the past few years.

An interesting question would therefore be how self-regulatory initiatives could gain some external effect. In other words, could a code of conduct adopted by representatives of certain actors influence or even determine the required behavior of actors that are not a party to the code of conduct? Although the recognition of such an effect would not guarantee an optimal sanctioning and enforcement of violations of the private norms, it will certainly contribute to the efficacy of self-regulatory schemes. One step further would be a situation in which the norms adopted, such as standards for on-line consumer protection, may become a professional standard whereby contravention automatically constitutes a fault. This would create a situation in which self-regulation becomes a key source of law complementary to the rules issued by the government and could perhaps even replace the latter. Could a situation thus arise in which trust or quality criteria for on-line communication and transactions become more than just the professional standard, i.e., a *de jure* standard?[89] An answer to this question requires a discussion on the legal status of self-regulatory initiatives versus third parties. Thus far, private law has been either very reluctant in debating the status under private law of self-regulatory mechanisms or has even fully ignored such a discussion. Given the prominent role of self-regulatory mechanisms in an on-line environment, it appears high time that such a debate is put on the agenda.

### *2. Facilitating action*

Legislation is not the only instrument of governments for regulation. In fact, they have a large variety of actions that may stimulate self-regulation or that can steer self-regulation in a direction that conforms better with the criteria for self-regulation. For instance, governments 'can assist in analyzing systemic problems in an industry and in facilitating the design of a self-regulatory response to address those systemic problems.'[90] The establishment of study groups or task forces, either directly or indirectly, for instance, through financial incentives, is an obvious way to stimulate self-regulation; the Dutch government's stimulation of the Electronic

---

[89] Prins & Schellekens 2005.

[90] <http://www.selfregulation.gov.au/publications/TaskForceOnIndustrySelf-Regulation/FinalReport/isr_part2-07.asp>, conclusion 35.

Commerce Platform is a good example of this,[91] as is the establishment of a public-private program on vulnerability on the Internet.[92]

In order to enhance the fairness of self-regulation, governments may also promote the interests of insufficiently represented or vulnerable groups,[93] for instance, by encouraging the self-regulatory parties to include representatives of consumer, human rights, and privacy organizations. Another procedural action is to facilitate some sort of monitoring mechanism, for example, a review or monitoring committee that checks whether the self-regulation complies with its own rules or with the general criteria for self-regulation (see section 5.4).

Perhaps most the important point is facilitating international adjustment: 'Government is uniquely placed to promote international cooperation and harmonization of self-regulatory initiatives.'[94] Many of these initiatives, after all, are national in character, resulting in an international kaleidoscope of potentially widely diverging rules. Moreover, since many ICT activities cross borders, it is a serious shortcoming when self-regulatory provisions are not applicable to users who are not subject to these rules. Therefore, it is important to pay attention to the international adjustment of self-regulatory programs, including trying to achieve co-operation between several countries to ensure effective enforcement of self-regulation. International adjustment can be achieved at different international forums, such as the OECD,[95] the Council of Europe, OAS and ASEAN, the UN,[96] or the ICC. It is not so much achieving regulation itself at these levels that is relevant in this context, but agenda-setting and awareness-raising: if sufficient attention within these international forums to diverging rules that emerge in a certain sector will be an incentive for market parties to work together to try and adjust their self-regulatory activities internationally.

### *3. Additional actions*

#### *3.1 Raising awareness*

One of the prime criteria for self-regulation is awareness, for in order to understand self-regulation and play by these rules, users must be aware of the existence and

---

[91] See <http://www.ecp.nl>.

[92] *Beleidsnota Kwetsbaarheid op Internet (KWINT)*. Kamerstukken II, 2000/01, 26 643, no. 30. The purpose of the KWINT program is to develop practical solutions for companies, citizens, consumers, and government, for a better protection against certain risks of Internet use: continuity of the Internet in the Netherlands, denial of service attacks, data integrity, authenticity, transparency of the Internet, abuse by personnel, and the exclusiveness of information. See <http://www.kwint.org>.

[93] See *supra* n. 17, at p. 181.

[94] <http://www.selfregulation.gov.au/publications/TaskForceOnIndustrySelf-Regulation/FinalReport/isr_part2-07.asp>, conclusion 37.

[95] See, for example, OECD Working Party on Information Security and Privacy, *Report on Compliance with, and Enforcement of Privacy Protection On-Line*, 12 February 2003, JT00139173.

[96] For example, the European Commission promoted the awareness and international co-operation against spam at the UN level for the World Summit on the Information Society in December 2003.

substance of the self-regulation. Governments can stimulate educational activities targeted at enhancing awareness. For example, the French Commission Nationale de l'Informatique et des Libertés (CNIL) has put a substantial information package on various aspects of spam on its web site.[97] The information package contains the results of its e-mailbox experience and the cases referred to judicial authorities, but also basic guidance on how to prevent spam, information on how to report spam, references of users' associations active in this area, etc.

Several government parties may be involved in the promotion of awareness: supervisory authorities, consumer protection agencies, ombudsmen, et cetera. These parties should focus on various steps to be taken, such as providing information about prevention and enforcement (do's and don'ts), users' rights, and complaint mechanisms. These awareness activities should not only be through web sites, but also through other means to reach the various audiences targeted, such as speeches, interviews, and e-mail alert services. Of course, governments carry only partial responsibility; involvement of industry and consumer associations is equally essential for raising effective awareness.

*3.2 Enhancing enforcement*

Another essential criterion for self-regulation, and the one in which government involvement may be most called for, is enforcement. Enhancing enforcement in various ways is one of the instruments the Dutch government mentioned for government action: 'cooperating in enforcing self-regulation, as for instance already happens with the Child-Porn Hotline'.[98]

An example is a project of the International Marketing Supervision Network (IMSN) that has resulted in a web site to gather and share complaints about cross-border electronic commerce;[99] among others, the Mexican Federal Consumer Protection Agency (Profeco) took part in this activity.[100] Government may also facilitate 'more interventionist' dispute resolution 'where businesses may be dealing with a large amount of complaints and/or dealing with complaints of a more serious nature', in which case 'an external dispute resolution scheme may be appropriate. An independent body capable of adjudicating and exercising sanctions can further strengthen an external dispute resolution scheme.'[101] Of course, governments can always provide legal backstop enforcement: 'The Code of Practice adopted by the

---

[97] See Commission Nationale de l'Informatique et Libertés, *Results of the Initiative Taken by the CNIL in Relation to Unsolicited Electronic Communications,* <http://www.cnil.fr/uk/Doc/CNIL-PR-spamming-VA.pdf>, February 2003.

[98] See *supra* n. 17, at p. 181.

[99] <http://www.econsumer.gov>.

[100] As mentioned in OECD Working Party on Information Security and Privacy, *Report on Compliance with, and Enforcement of Privacy Protection On-Line*, 12 February 2003, available at < http://www.olis.oecd.org/olis/2002doc.nsf/43bb6130e5e86e5fc12569fa005d004c/26eb7e5a8a723451c1256cad004fbf8d/$FILE/JT00139173.PDF>, p. 10.

[101] <http://www.selfregulation.gov.au/publications/TaskForceOnIndustrySelf-Regulation/FinalReport/isr_part2-06.asp>.

Fruit Juice Industry is supervised by an Industry Compliance Committee. Ultimate sanctions are law enforcement by the appropriate government regulatory bodies should the self-regulatory scheme be ignored or flouted by participants.'[102]

## 5.6 What Should It Mean?

Although they are often (implicitly) contrasted as opposites, self-regulation and legislation are not mutually exclusive. The existence of self-regulatory systems does not prevent the national or international legislature from taking initiatives. In fact, having studied a plethora of self-regulatory initiatives, we may even conclude that pure self-regulation is rare, and that most self-regulatory initiatives in some way have a back-up in formal legal rules or in other public regulatory instruments.

Therefore, 'the starting point is self-regulation' creates a wrong impression of a preference for (pure) self-regulation over government regulation, which effectively is a false dichotomy. The starting point should rather be turned around: 'ICT regulation should not be purely a government activity, but should also involve private parties.'

In what cases would this be a good starting point? We have listed several criteria to judge when and to what extent self-regulation can be considered a viable addition to government regulation. Primary criteria that should be safeguarded are fairness, inclusiveness, and compliance. Also, transparency, legal certainty, efficiency, and the context of the regulation play a part in deciding to what extent regulation should involve private parties. This means, for instance, that domains in which fairness and inclusiveness are at risk, for example, because fundamental rights and vulnerable groups are involved, and in domains where self-compliance is not a given, government regulation should be more prominent than self-regulation. Conversely, in non-contentious domains where there is a reasonable balance of stakeholders who have an interest in complying, there is ample room for private parties to self-regulate, with relatively little government activity in the background. It is noteworthy that many of the criteria for self-regulation are procedural rather than substantive ones.[103]

Supposing that some form of self-regulation is indicated, the next question is how private parties should be involved and what role there is for the government. The ways of involving private parties are numerous: codes of conduct, seals and trustmarks, hotlines, standardization, and incorporating norms into technology are some examples of regulation undertaken by the private sector. Governments can

---

[102] Ibid.

[103] Cf., Prins & Schellekens 2004, who call for the development and analysis of procedural criteria, such as: Do all interested parties get a relevant hearing in any way? Is there some form of a self-reflective mechanism to understand earlier mistakes and challenge and review of earlier adopted norms? Is there an opportunity for a wide range of views and arguments to be discussed in an open dialogue by different stakeholders rather than a narrow selection determined by market forces?

back-up such initiatives in a variety of ways, for instance, by enacting codifying, backstop, framework, procedural, or liability legislation. They have other instruments as well to protect fundamental values such as fairness and inclusiveness: they can stimulate fair procedures in self-regulatory processes, enhance international adjustment, or facilitate monitoring mechanisms. Moreover, they have a task in raising awareness and in enhancing enforcement, so that self-regulatory rules are indeed followed in practice.

This means that the best way of reading the starting point is: 'Co-regulation is the starting point'. This is not a revolutionary conclusion, nor is it particularly helpful in solving real-life regulatory problems in the field of ICT. The starting point says little about when and how what forms of co-regulation are to be chosen. This chapter has tried to give some clues for putting this starting point into operation, with a checklist of criteria and an indication of regulatory instruments. Still, numerous questions and trade-offs remain. A few of the questions that merit further analyses are the following: under what circumstances do self-regulatory rules have an external effect? To what extent would courts be willing to take into account self-regulatory standards to hold private actors liable? Should 'harmonization' of self-regulatory initiatives be considered to enhance legal certainty and international adjustment? What instruments are best suited for enhancing the fairness and inclusiveness of self-rule-making, and what instruments can best ensure self-compliance? Only when we have satisfactory answers to such questions can we really say that 'the starting point is co-regulation'.