

Chapter 2

Evolution, Implementation and Practice of Internet Self-regulation, Co-regulation and Public–Private Collaboration

Cormac Callanan

Abstract This chapter examines the practical evolution of Internet self- and co-regulation and reflects on the current approaches in the fields of cybercrime, cybersecurity and national security. First, it provides insights into the development of self- and co-regulatory approaches to cybercrime and cybersecurity in the multi-stakeholder environment from the beginning of the Internet service provider industry. Second, it highlights the differences concerning the ecosystem of stakeholders involved in each area. Detailed analysis focuses on existing forms of collaboration, highlighting the differences and difficulties in leveraging the forms of cooperation and successful approaches from one area to another. The last part analyses the problems of multi-stakeholder approaches. It will also examine the drawbacks of the existing forms of public–private collaboration, which can be attributed to a specific area (cybercrime, cybersecurity and national security). Ultimately, this chapter provides some suggestions with regard to the way forward in self- and co-regulation in securing cyberspace. It offers unique insights into the role of Internet industry in combatting cybercrime, improving cybersecurity and supporting national security. It identifies the current practical and economic limits on cooperation between industry and state agencies and describes the balance between human rights/data privacy and crime investigation. It concludes with the challenge of state over-reaching their mandate—when national security becomes political interference in human rights.

Keywords Self-regulation • Co-regulation • Public–Private-Partnerships • Internet-Industry • Illegal Internet Content • Harmful Internet Content

2.1 The Birth of Self-regulation

2.1.1 Introduction

After 15 years of operation, there are still huge misconceptions and confusion surrounding the areas of self-regulation and co-regulation in the Internet industry. This confusion is shared among experts in the field and frequently complex debate can collapse into total disarray when it is discovered that those present have very different meanings and expectations on the area of self-regulation. Chapter 1 extensively describes the evolution and changing nature of the legislative, regulatory approaches to cybersecurity and cybercrime and the role of public-private partnerships. Whereas there are many research documents describing the different strategies to these partnerships, they sometimes seem to suggest that there was a clear long-term strategy being followed by the government and by industry representatives. However, whereas there were short-term tactics adopted relating to specific issues, much of the progress on improving cybersecurity and combating cybercrime was achieved from the constructive tensions which existed between government and industry at the beginning and then later between the variety of stakeholders actively engaged in cybersecurity and cybercrime issues. Chapter 1 rightly notes that governments were under pressure to “do something” (Sect. 1.5.2 p. 34) and this was a fundamental aspect of the early days of public-private partnerships. There was pressure to “do something” and the challenge was to determine what was that “something”, who would “do” it and would it be enough to address rapidly evolving Internet challenges.

It seems appropriate therefore to start this review of self-regulation and co-regulation by looking at the definitions, consider the reason behind the persistent confusions and attempt to clarify the historical trends that have evolved to current self-regulation approaches. It started because of the government policy to support and encourage information society services and not create a chilling effect on Internet services by introducing heavy-handed regulatory issues. The main differences between styles of self-regulation are based on the stakeholders involved. It can be divided into five categories that include individual, company, industry sector, guided by regulation (sometimes called co-regulation) and multi-stakeholder.

2.1.2 Individual

Companies are led by individuals who decide on their own interpretation of what would be appropriate policy or ethics for their organisation. They choose this based on the assessment of the consumer base and the changing needs of the company over time. The strength of this approach is that there is strong commitment to self-regulation but the weakness is that it varies over time, does not have a consistent approach over time and changes as senior managers change.

2.1.3 Company

Self-regulation is performed at a company level where decisions are made by the company management board which decides what elements of self-regulation are appropriate for their organisation based on the company ethics profile and understanding of corporate social responsibility (CSR). The strength of this approach is that there is strong commitment and greater consistency over time. In addition, the organisation knows more about the specific area of technology and how it can be abused and the possibilities for positive action. The weakness is that it is directly related to current market conditions and is more relevant for large multinationals than small (less than 100 employees) organisations. This system has the challenge that there is no consistent approach for all organisations which can be monitored and measured for effectiveness. The policies are not always published and they can vary significantly between countries of operation. Another weakness of this approach is that it can turn important societal issues into competitive market positioning activities.

2.1.4 Industry Sector

Self-regulation is determined by a coordinated industry approach. Individual organisations come together to discuss and agree a common approach to specific issues. Once agreed, these areas of common interest can be implemented by a shared organisation with a mandate to implement the agreed protocols or to represent the group of organisations in an agreed manner. There can be agreed membership procedures, funding structures and regular meetings to share knowledge and concerns and agree policies. There can be common codes of conduct and ethics, and there can be complaint procedures against the activities or behaviours of one of the members of that shared organisation. The strength of this approach is the common consistent approach by a range of industry players, which is a powerful response to agreed issues. The weakness is that it takes longer to agree a common profile on certain issues. There can be issues that have different levels of impact to different members and therefore have different levels of urgency. There is also a concern that the industry body is only interested in the best interests of the industry and not in the broader needs of the society which can lead to concerns about transparency and accountability. In addition, many countries prevent corporations to act in collusion in the marketplace and therefore, the areas of common interest need to be very narrowly focused and clearly focused on areas of societal interest and not on business behaviours or the potential unintentional creation of a cartel.

2.1.5 Guided by Regulation (Sometimes Called Co-regulation)

This approach brings together the role of government and the role of the industry sector whereby there is a role for government stakeholders to participate in the discussions to form policy for the industry sector. This can be further enhanced by the implementation of legislation on which the fundamentals of industry responsibility are detailed with motivations and sanctions clearly outlined. Often these regulations or legislative initiatives are first discussed with the industry and designed to have reasonable and fair impact on all industry members with a clear responsibility for action and liability for non-compliance. The strength of this approach is that there is a consistent approach to (self-) regulation over time and that the industry has external oversight to ensure progress on issues causing major inter-organisation disagreement. In addition, there is a wider range of expertise available to state organisations sharing their collective knowledge and experiences to develop the best possible response. A major weakness is that it is difficult to respond to issues in a timely manner and that there might not be an adequate range of competencies in the industry or state stakeholders.

2.1.6 Multi-stakeholder

This multi-stakeholder grouping takes the strengths of the previous groupings and expands the stakeholders to include experts from a range of other areas of society. This brings a broader range of expertise to the discussions and responds to issues about transparency, accountability and oversight of industry behaviour. However, the downside of this approach is that there is a larger, diverse grouping of experts which can take longer to be fully apprised of the range of aspects of an individual problem, and there is an even wider range of political, social and personal interests that is brought into discussion. In addition, those affected (both financially and legally) by the final decisions are often the minority voice in the debate.

It can be seen that there a wide range of approaches to self-regulation and co-regulation which offer different levels of transparency, accountability, oversight and effectiveness. These different approaches evolved over time and continue to be in use today. Many of these approaches are used in parallel and can be very confusing to the observer. To understand how these approaches worked in practice, the evolution of Internet services needs to be considered.

2.1.7 Background

In 1996, I had just completed the sale of my Internet company called IEunet (EUnet Ireland) in Dublin, Ireland. My business partner and I had started the first commercial Internet business in Ireland, recognising the importance of the Internet to business, in 1991. Business was hectic with Internet access provided over analogue modems for services such as Gopher, email and FTP. The arrival of the web protocols in 1991 had a dramatic effect on traffic profiles. We started the company with modems operating at 1200 baud, and by the time we sold the company in 1996, the modems were operating at 57,600 baud and the international bandwidth was very expensive. ISDN services were also becoming popular. Broadband to the home was still a distant dream. Self-regulation in those days was unheard of and mostly it was based on internal company reactions to changing customer requirements in problems identified in the network. So the first understanding of self-regulation was that a single company would endeavour to ensure that their view of acceptable moral and legal standards was enforced against customers of their service.

Already the arrival of home user consumers onto the Internet was causing significant impact. The user profile for these users was quite significantly different. Business users had a clear business focus and interest in a reliable service as the primary interest. They accessed the Internet during the day using computers controlled by their business, and the contact between our network and theirs was often performed between technically competent personnel in their IT department and our network operations centre engineers. During this phase, telecom companies were not paying attention to the Internet since they could neither understand the business model of the Internet nor the use of the technologies such as freeware and shareware neither purchased nor supported by tier-1 software and hardware multinationals. Traditional telecom companies focused their service sales in the data carrier area on X25 and X400 with clear, expensive charging models. Equipment to implement X25 and X400 was expensive and data were priced on packets sent and received (international sharing). However, it was very true to say that a telecom company depended on the flexibility and reliability of their billing systems to be successful. Such systems tracked resource usage and, more importantly, ensured that all such usage was charged to the correct customer.

The arrival of the HTTP protocol (the web) and the first mass-market versions of NCSA Mosaic in January 1993 had a dramatic effect on the Internet businesses and changed the Internet forever.

My company had a small and growing turnover with a loyal customer base accessing a range of core services. Around 1992, there was increasing demand for online connectivity to Internet services with increasing requests and sales of dedicated leased lines from customers to connect to the Internet and to be online 24/7, enabling the provision of business web services by our customer base. Facing

into substantial investment to maintain sufficient international bandwidth at a time when telecom companies across Europe were still state-owned monopolies, and increase staffing to support the growth, we had the opportunity to sell our business to a company who later sold the business on to a telecom company in the next years. The arrival of online services and phenomenal interest in the Internet attracted the attention and interest of traditional telecom operators.

2.1.8 Content versus Traffic

Before 1993, the primary services on the Internet were mainly text focused and included email, Usenet News and Gopher. Graphic image files could be exchanged between users by breaking them into equal chunks of data like pieces of a jigsaw puzzle transmitting them in different news or email messages and then re-combining the pieces back together to recreate the original image. There was dedicated software that would dissect and reconstitute a range of files to/from an individual document.

2.1.9 Usenet News

Usenet News was where active publicly visible self-regulation began with technical blocking and content assessment. This is explained in more detail in the next chapter but is introduced here. Usenet News had very high volumes of traffic consuming as much as 40 % of international bandwidth and storage capacity on the core network systems. It took up a significant amount of operations engineers' time to support and maintain the smooth flowing information content and the increasingly large number of news topic. Each customer could select which newsgroups to include in their news feeds and also which ones could be blocked and not updated. In the beginning, newsgroups focused on sharing technical tips and tricks between computing specialists and sharing free software tools (using chopping-into-chunks and reconstruction). However, over time, due to its success in the technical area, newsgroups were created for hobbies and crafts (fishing, chess, gaming, knitting and cooking) and for discussion and debate on a wide range of social issues (poverty, global warming, air travel, politics and sex).

Newsgroup traffic volumes across international lines and local disk storage were constantly monitored. The quality and capacity of an ISP and the number of days of newsgroup storage were among the key performance criteria when selecting an Internet service provider. A flurry of activity and vibrant interchange of ideas on newsgroups over a weekend or holiday could easily consume over 90 % of international bandwidth or over 90 % of available expensive disk space, thereby blocking other activities on the systems. In the beginning, users would usually decide to take all newsgroups and, then over time, in order to reduce bandwidth

consumption and storage requirement, they would reduce the number of days stored and updated and then reduce the range of newsgroups over time. Several newsgroups including newsgroups related to software development (alt.binaries, alt.binaries.images, music, etc.,) generated large volumes of large messages since some documents/programs could be broken into over 50 individual message chunks. As a result, it was easier over time to determine which specific newsgroups consumed the most resources. This is my earliest memory of the beginning of the online sex/pornography debate.

The newsgroup hierarchy¹ had many groups dedicated to sex-related content including but not limited to pornographic material. Initially, it covered discussions about sex with separate discussions about homosexuality or celibacy or pregnancy or sexual health. Some of these newsgroups were moderated but the majority of the newsgroups were not. The issues of homosexuality or abortion were topics of passionate debate in Ireland during those days and our company was apprehensive about the legal standing and potential liability of hosting newsgroup discussions on these topics. It is not a surprise therefore that sexual content and the issue of legality were considered as intrinsic to Internet self-regulation evolution. It is not true to say that these issues were constantly debated inside the company, but the issue of the legal uncertainty around some type of sex-related content was occasionally debated over coffee. I have no recollection of any legally qualified professionals at that time having sufficient knowledge or understanding of Internet technologies in order to be able to form coherent comprehensive legal advice based on the state of the Irish legal system. It was not realistic for the company to have a clear legal understanding of what was or what was not legal on online services.

By 1992, there were over 15,000 different newsgroup titles divided into different news hierarchies, and bandwidth consumption became a serious concern for the Internet backbone systems. It was decided that the company needed to conserve bandwidth by reducing the number of newsgroups being carried and therefore accessible to consumers. This then created a debate about which specific newsgroups would be “dropped” (the word “blocked” had not been invented yet!). This started the debate on two other issues which became major issues for the future. These are consumer profiling and freedom of speech. My Internet business sold services primarily to companies, but a small number of customers were individuals who had adopted the Internet early.

There were two ways to access news—one way was to take a news feed and select/identify which newsgroup hierarchies or even specific newsgroups to subscribe to. The contents of these newsgroups were then transferred to the customer’s system for later reading or expiration. There were no records available on our system about which individual news items were read or archived by the customer.

¹Additional technical details is available on <http://en.wikipedia.org/wiki/Usenet> (last accessed 11 Dec 2014).

2.1.10 Log Records and Charging

In the second access method, a customer would access the hierarchy stored in our systems using newsgroup client software. These systems would leave log records to identify which newsgroup had been accessed and which specific news items were read by each consumer. Broadly speaking, no one was deliberately analysing these logs to monitor individual organisations or people. The log files were designed to determine errors with the communications. Many log files were very vague or inaccurate and were used to diagnose specific technical performance issue. However, our ISP charged users a flat rate for a news feed and separately charged in volume groups for email transmission and receipt. We therefore used the log records to determine the volume and quantity of emails sent and received per customer. In fact, we became so good at this that we generated monthly summary usage reports for our customers which were sent with their monthly invoice! We would then plan future invoicing structures with our customers based on these usage reports generated by detailed log analysis. At this phase of evolution, therefore, we became aware of the level of business information and personally or business-sensitive information, which was being recorded by the core network systems, and the need for security, privacy, confidentiality and data protection acumen across the organisation. We instilled in all staff the need for respect for privacy in a similar way as a bank would train new staff. The concern at this time was to build trust and confidence with users and businesses to encourage adaption of Internet services. It was by no means certain that Internet services would survive and evolve.

Many of the Internet structures—DNS, ip-allocation, international routing agreements—were still based on academia and managed by highly competent, motivated individuals on a voluntary basis. It was not obvious which Internet services could be productised and priced at acceptable levels both for the consumer and the business selling the service to be adequately profitable. In fact, the concept of selling access to the Internet was frowned on by many of the grandfathers of the Internet who were aghast on the issue of allowing commercial entities to pollute the purity of online research depending on the Internet, or shocked at the concept of selling Internet like it was a product or a commodity—almost like prostitution!

2.1.11 Traditional Telecom Services

On the other side of the debate, the national telecommunications operators operated in a monopolist environment. Usually a national telecommunications company was owned, operated and directly controlled by the state and was licenced, regulated and authorised to exclusively sell telecommunications services to the general public. Phone lines were not readily available across the Irish state and often incurred delays of over 6 months to get a phone line installed. All telecom workers were

state employees and were required to sign the official secrets act when they started their career in telecommunications. These telecom operators sold several core services including voice and data on a monopoly basis.

Many of these telecommunications services had different levels of volume purchasing from a single voice channel/line at the low end and over 30–100 voice channels at the high end. In the data area, one could use an X25 circuit across a dedicated phone line or the cash-rich organisations could purchase dedicated leased lines from telecom to connect your business to your customer or perhaps your headquarters. Dial-up modem connections or dedicated leased lines from telecom were the only ways that users could connect to the Internet. We offered Internet services and our connection to the global Internet was through a leased line to the UK and later a dedicated leased line to the central EUnet network operations centre in Amsterdam, thereby linking us to other countries connected into Amsterdam across Europe. EUnet then operated a fixed line to the USA. The cost of an international telecommunications link was exorbitant. We worked to ensure the maximum efficiency and usage of these links and they were the major expenditure of our business. If one includes the rental costs of dial-up phone lines (which reached 30 lines at one point) and the other lines installed on behalf of customers, the overall expenditure on telecommunication by my company was enormous. We were also totally dependent on those links for business connectivity and when links failed, we strived to maintain a professional, courteous relationship with Telecom Eireann who supplied and maintained these services for us. By the mid-1990s, it became clear to telecommunications companies that X25/X400 services were faltering and failing to achieve significant market penetration or acceptance. It also became clear, with the phenomenal growth of the web technologies released to the world in 1992, that the Internet usage was increasing exponentially across the world and challenging and undermining established Telecom product sales and services. This became a problem when telecommunications operators were forced to accept that they needed to embrace the Internet and then begin offering a basic range of Internet services to their client base. Although there was a range of in-house skills available to offer basic communications services such as modems, ISDN and dedicated leased circuits, there was less skill available to manage the TCP/IP protocols or the higher level applications such as news, email and web.

Telecommunications companies had a long history of working closely with state agencies and implementing government policy since they were owned and regulated by the government. Employees were considered as state employees. This relationship became very influential in the growth of self-regulation initiatives across Europe. However, telecommunications companies were more comfortable with a clear government-mandated regulatory environment with which they had a lot of experience and familiarity. On the other hand, the new Internet companies had little experience of self-regulation, had suffered first-hand effects of a monopolistic telecommunications market and expected that a regulatory-driven environment would be biased towards telecommunications companies and against creative, evolving information society services coming from the Internet. This tension became an essential element of the evolution of self-regulation.

2.1.12 Open Telecommunications Market

Although the national incumbent telecom provider still had a monopoly to offer network connections and home voice telecom services, the laws and regulations in the area of data services were not so clear. Organisations could access international leased lines by leasing a line locally to a distribution point and gain access to international bandwidth through that point. These would use the services of a growing range of international carriers—often the national carriers in other European countries competing with each other on international services. Once a dedicated leased line was purchased by a company in Ireland, there were few restrictions of what services or communications protocols could be implemented on that line. For example, one service provided by my company was Internet services and others included offering pay as you use international voice services. This bypassed local regulation by first requiring a customer to dial a local number, enter a pin code and then input the desired international number. These type of services undercut the profit margins of the national telecom company and drew direct attention to the major technological upheavals being experienced by the telecom sector across Europe. In summary, although telecom was a monopoly in each country across Europe, there was a wide range of technological options available to encourage increased competition between national carriers competing international and other embryonic operations at a national level. As the market became more open, there was increasing business competition in what became known as “other licenced operations—OLOs”, which is still in use today.

2.1.13 Dropping Newsgroups

During 1993, our international bandwidth was insufficient for the volume of traffic, incurred heavy usage on a 24 × 7 basis. Since we focused on business clients, we managed the traffic to offer highest possible quality of service to the customers during office hours and reassigned system requirements to out-of-office-hours slots. This included system backups, system upgrades and even newsgroup transfers to/from our international providers. This traffic shaping was a crude human-managed manual activity that strived to achieve the most efficient usage of available resources—bandwidth and storage. This initiative drew our focus towards the newsgroup system and regular technical monitoring and reporting. We monitored fluctuations on newsgroup message volumes and fluctuations on message size. We noted the growing number of newsgroups titles and the increase in newsgroups of a social nature or dealing with recreations such as football, volleyball, basketball, fishing, cycling and swimming. The newsgroup system was a subject of every management meeting, and most discussions were about ways to minimise its effect on our scarce and valuable system resources. The company continued the traffic shaping policy by providing different level of services between different sections of

the newsgroup hierarchies—to improve the overall impact on the quality of services. We decided that we would only update some high-volume hierarchies during night-time hours but ensure some hierarchies in regular use by our customers continued to be updated during less busy traffic times throughout the day. Most of the customers accepted and understood this change as an overall service improvement. Since our service targeted business customers, the primary target areas for newsgroup efficiencies were focused on those non-business, socially focused newsgroups. A clean differentiation was not always possible, and we sometimes received requests for specific newsgroups to be updated more frequently which we accommodated.

However, newsgroup volumes continued to grow, and we eventually decided to drop some newsgroups completely from our service. The first newsgroups we dropped were those groups with very large volume of very large size messages causing a noticeable spike in using system resources. A cursory examination of the title/name of these newsgroups indicated that the material related to explicit sexual content including both images and text. This type of content incurred phenomenal growth on the Internet, and this was a wide range from soft-porn images to what is known as hard-porn and even what later became known as illegal content. We stopped carrying these newsgroups. Publicly, the explanation for this decision was the significant impact on scarce system resources caused by the volume of content in these newsgroups. In addition, since the business sector was our primary target market there was no interest by these customers in these newsgroups. Privately, we lived in a country where printed pornography was banned, homosexuality was a criminal offence and contraception was strictly regulated. Our business was licenced but arguably in a very unclear legal area of telecommunication services potentially restricted by the state. We were concerned that the additional complexity of hosting content (for a business service of little business benefit) might draw undesirable attention from various state agencies. Therefore, when we made our public announcement among many other technical updates, we wondered whether we would receive any complaints from our customer base or even debate of the newsgroups we selected to be no longer carried on our service. There were no major concerns expressed from any of the customers although it was noted by many that the range of newsgroups being carried had changed. Many customers had already noted the increasing volumes and the subsequent impact on their own resources and saw the changed list as an opportunity to regularise their own systems and reached a similar conclusion to the content choice.

2.1.14 Embryonic Self-regulation

At this time, around 1993–1994, we had faced the difficult choice of basic, elementary self-regulation and faced up to specific decisions relating to content. These two issues were the major challenge found by the Internet service providers across Europe. Most of the owners and managers were not adequately trained or skilled in debating the

challenging nuances between freedom of speech and human rights or not carrying certain type of content—where a choice was possible. Most of the Internet service providers believed that the service they provided was defined according to their own choice. They did not accept or acknowledge that they had a public duty to carry content without personal bias to different types of content. In these early years, they knew nothing of the debates around the net-neutrality and managed those Internet services as their own little dominion. There were some balancing aspects. Traditional telecom operators were not held liable for content or behaviours exercised using their technical infrastructure. For example, bomb threats, suicide or harassment phone calls were not considered an issue of liability for the telecommunications operator but of the person who committed the act. As long as the operator played no active role in causing those phone calls to occur, it was considered that they were exempt from liability. This was known as common carrier status. Many Internet service providers assumed that they would be considered as common carriers by operators, regulatory authorities, governments and in the Courts if there was any legal challenge. There was a corollary to this issue of common carrier status, which became a major issue in later debates on self-regulation. Whereas an ISP would not be held liable for content carried on their networks which they had not initiated or directly requested, they might introduce liability for themselves if they voluntarily chose to take steps to manage or control the large volumes of diverse content and activities that take place on their networks. In other words, if you take and accept any responsibility for content—no matter how minor—the protection afforded by the common carrier status might be considered as waived.

Much of all these legal musings and ramblings were not based on specific facts or legal texts or a deep academic understanding of international human rights law or commercial contracts. It was based on hearsay, collected wisdoms and shared discussions among staff in the international EUnet networks and issues which arose for different network members during these early developmental years of Internet services. I remember being asked by EUnet to take responsibility to specify and define the exact descriptions of the services which we were selling to customers across Europe in order for us to learn more about the possible options, charging models, revenue models and actual cost for each service and variation in each service. This was a mammoth task which succeeded in highlighting the large variety of services and the complex range of options on offer across Europe. It is reasonable and fair to note that most of the members of EUnet were more focused on business growth and overcoming daily technical challenges than philosophical debates relating to content. Although it was increasingly clear that Internet services were experiencing exponential demand, it was not clear if there was a financial/revenue sustaining model, which would work for the individual member of the EUnet network. Although there were occasional debates about content issues, these focused almost exclusively on the impacts relating to service efficiency and on the financial bottom line rather than the nature of the content itself. Other members of the EUnet network did not have any technical, or system or network resources in carrying a full newsgroup feed and did not have to make a choice over which newsgroups to drop and which to carry. So they continued to carry and distribute a

full newsgroup feed until newsgroups became the first open battle in the area of self-regulation. This occurred in the UK and is described in detail in the next section. In Ireland, the newsgroup service continued with the reduced selection of newsgroups. When we later purchased extra bandwidth, the newsgroup list was restored to a full service for a short period of time, but as the additional bandwidth also came under pressure from traffic volumes, the news feed was reduced again.

2.1.15 Anecdote

Almost a year after this policy was initiated, I received a request for a meeting with one customer relating to newsgroups. I remember being very curious how the meeting would unfold. I incorrectly assumed that we would discuss the selection process we had used and whether there were any hidden biases or phobias in favour of or against one religious morality or social ethos which was a constant issue of public discourse throughout the 1980s and 1990s in Ireland. The person I met was a young man dressed like a student. He was quiet spoken and slightly nervous. The theme of the meeting was the newsgroup policy. To my surprise, he understood that we had blocked some groups which seemed to accept/support/encourage child sex abuse; he also noted that other content relating to adult content, homosexuality, etc. was morally difficult to determine. He explained that he had come to request me to restore one newsgroup to the unblocked lists. Whereas he accessed this newsgroup on our service before, he could still access the newsgroup through international news services. He explained to me that the group he was referring to might appear similar to the other newsgroups in that area. However, it focused on supporting victims of child sexual abuse and coping and recovery strategies. I was told that he had been abused when he was younger and was now dealing with the impact and effects on his life, and this newsgroup helped him share with others and learn from others who had suffered similar pains to him. After he left my office, I was quite taken by his story and I remember reflecting on the complexity of online content issues and the complexity of assuming the mantle of guardian of moral rights without oversight, transparency and accountability. It was clear to me that the issue of content was a major challenge for the Internet. It was also clear that the challenges were diverse and divisive with many conflicting debates with few clear obvious solutions. All these early minor forays into issues surrounding content and self-regulation were the beginning of a large time of my life spent debating and encouraging practical solutions for *illegal and harmful content* and activity on the Internet.

2.1.16 Conclusion

In the early 1990s, the benefits of Internet access for business were clear. Email began to replace facsimile (fax) and there was incredible growth in free software

tools available on the Internet. Microsoft had initially denied that TCP/IP protocol had any relevance to their business, later recanted and released TCP/IP support in the NT 3.1 release. Users on Windows 3.x and Windows Millennium needed to install extra software to use TCP/IP and dial-up services to use the Internet. In spite of the obstacles facing users of mainstream operating systems, the Internet was enthusiastically adopted and grew out of academia spread into business services and had finally been taken into the home. The price of personal computers was high, modems were expensive and reasonably priced Internet software was difficult to find and configure. The first home users were users who had access at work and were instantly convinced of the importance of Internet access to communicate with colleges around the world, and by using Usenet News and Gopher could stay up to date with the latest hardware and software developments. My company did not target home users, but we had several customers who paid expensive subscription to access the Internet from home. Some of these had the subscription paid by their companies. However, a company was started in 1993 called Ireland Online with a specific mandate to target home customers and small businesses. In the first years of their existence, they purchased their upstream connection from my company, but in the later years they purchased their own international bandwidth to the UK.

By the mid-1990s, the price of modems had dramatically dropped with the lower priced US Robotics modem at 21 Kbps speed in 1992. This speed increased to 38.8 Kbps and later 56 Kbps modems around the same time as 64 K ISDN lines from Telecom Eireann became available. However, the cost of international bandwidth had only reduced marginally since the telecommunications market was still a monopoly environment. The evolution of the Internet had reached a point where modems were now affordable, the software and hardware needed to access the Internet were more accessible and were also understandable by the ordinary user, and the HTTP web protocol was released to the world enabling easier dissemination of multimedia content on the Internet than ever before. With this wonderful availability of options, the drive towards Internet adoption accelerated and Internet growth patterns started to grow exponentially. It became an amazing stressful roller-coaster time of business growth, user expectations and demands and endless frustrations with slow networks, failing modem connections, long downloads and bandwidth utilisation charts which seemed to flatline at 100 % usage. My enduring memory of those times was the stress and the endless pent-up demand and the amazing new ideas that unfolded each day at work. It was an amazing time of technological creativity.

In 1996, the company was sold to a market investor and I stood down as owner and manager. The company had grown over 5 years to one of Ireland's leading Internet service companies. The societal challenges caused by content on the Internet were clear to see. There were daily technology improvements and Internet adoption figures continued to grow exponentially. The Internet was here to stay and brought a range of new challenges to the society. Society was not prepared for many of these.

2.2 Self-regulation Matures

2.2.1 Introduction

From 1996 onwards, self-regulation activities became more focused and were publicly debated with extensive engagement by intergovernmental organisations (Council of Europe, European Union, OSCE, United Nations, etc.), national governments and law enforcement. The subject of these discussions is related to the role of the Internet industry and the need for concrete practical action against concerns relating to the Internet. Unfortunately, there was a dearth of actual clear societal and governmental policies or a clear identifiable target of specific concern. The growing awareness of the volume of child pornography on the Internet became a focus of this concern and the common shared focus and interest of desirable direct action and effective response. Child abuse was not a new crime since it had previously happened in closed secretive environments, and before the arrival of images of child abuse (child pornography), the only way it was discovered and investigated was when sufficient trust was placed in the word of the abused child. The widespread creation and distribution of child pornography—the images of a crime scene—on the Internet had an enormously shocking impact on people around the world, and many Internet service providers chose to take steps to combat such content and activity.

2.2.2 Putting Structure on Self-regulation

On **24 April 1996**, at the informal European Council meeting held in Bologna, the European Telecommunications and Culture ministers identified the issue of illegal and harmful content on the Internet as an urgent priority. The European Council then requested the European Commission “to produce a summary of problems posed by the rapid development of the Internet and to assess, in particular, the desirability of Community or international regulation”.

2.2.3 UK French Letter

On **9 August 1996**, the Metropolitan Police Service in the UK sent out a famous letter² which became known as the “French letter” to all Internet service providers about pornographic material on the Internet specifically relating to newsgroup content and requesting that 133 newsgroups³ would no longer be distributed.

²<http://textfiles.com/magazines/CUD/cud0862.txt>.

³http://www.computerworld.co.nz/article/519610/british_police_list_133_obscene_newsgroups/ (last accessed 8 Dec 2014).

The letter shown in the box was a defining moment in the history of self-regulation. In essence, the Metropolitan Police Service had identified a list of 133 newsgroups which they believed were pornographic in nature and would likely be illegal under the obscene publications act in the UK. They acknowledge that the content in the newsgroup was continually changing and then requested the Internet service providers to monitor these newsgroups in order to “take necessary action against those others found to contain such material”. According to Richard Barry in the Independent⁴ on 2 September 1996, “the police argue that under the Obscene Publications Act and the Protection of Children Act, the ISPs are breaking the law and must act to stop the material from being accessed”.

This was a very interesting development in the history of self-regulation for Internet service providers located in the United Kingdom and across Europe since this was the first time that it had been suggested that they would be held liable for content they host or content they carry on their services. It was not clear how broad this liability would stretch, and at the time, there was significant concern that such liability would have a huge chilling effect on Internet growth and Internet adoption by users. It is worth noting that the letter referred to a broad range of pornographic content which was not limited or bounded in any way. There are a number of intriguing issues relating to this initiative:

- A national police force had taken upon itself the right and responsibility to request an Internet service provider not to distribute the contents of a list of newsgroups identified by the police and specified by name. It did not appear that this was implemented as a result of a specific government policy or mandate, but was an effort to enforce the rule that what was illegal offline was also illegal online.
- This introduced the role of police to proactively prevent potential online criminal activity with no direct engagement with the judiciary processes.
- It introduced the concept of notice and takedown relating to illegal content.
- Liability for the Internet service providers was linked to the concept of actual knowledge of illegal online activities.
- It was further stated that the list might change depending on the changing nature of the content of such groups and that the police expect ISPs to continuously monitor newsgroups and to remove those which contain illegal materials. This was a major concern since it suggested that the Internet service providers should proactively monitor their networks for illegal activity and raised the spectre of widespread pervasive monitoring with its obvious conflict with human rights.
- That an ISP would be considered the publisher of such material and therefore likely to be liable for publication of such content.
- It was implicitly suggested by the police that this was their understanding of what they considered to be self-regulation by the industry players.
- There was clear threat of enforcement if the request was ignored.

⁴<http://www.independent.co.uk/life-style/the-list-and-the-hysteria-1361446.html> (last accessed 8 Dec 2014).

Date-- 9th August 1996

METROPOLITAN POLICE SERVICE

Clubs and Vice Unit
Charing Cross Police Station
Agar Street
London WC2N 4JP

Telephone: 0171 321 7752
Facsimile: 0171 321 7762

To: All Internet Service Providers

Dear Sir / Madam

Pornographic Material on the Internet

Further to the seminar held at New Scotland Yard on 2nd August I enclose, as promised by Superintendent Mike Hoskins, a list of those Newsgroups which we believe contain pornographic material.

We have attempted to confirm that the Newsgroups listed currently contain this offensive material but as you will be only too aware the content is continually changing and you will need to satisfy yourself about the nature and content before taking any action. Furthermore, this list is not exhaustive and we are looking to you to monitor your Newsgroups identifying and taking necessary action against those others found to contain such material. As you will be aware the publication of obscene articles is an offence.

This list is only the starting point and we hope, with the co-operation and assistance of the industry and your trade organisations, to be moving quickly towards the eradication of this type of Newsgroup from the Internet. At the seminar we debated the means of maintaining an up to date list and you will recall that ISPA volunteered to pool information and assist in this initiative. However, we are very anxious that all service providers should be taking positive action now, whether or not they are members of a trade association.

At this time, there were approximately 1.3 million⁵ Internet subscribers in the UK. There was real concern with European ISPs that this national enforcement action might be applied to the Internet service providers across Europe. Jim Dixon from VBCnet⁶ in the UK stated that “*While we do not disagree that the articles in some of these groups are often objectionable, we disagree in principle with this form of censorship*”. He urged all customers to make it clear “*why these news groups have been withdrawn and we urge you to contact your MPs and the media about this arbitrary action by the police. If there is no protest, if a precedent is established, the UK Internet is going to fall under the control of the Clubs and Vice Unit at Charing Cross Police Station*”. The list is shown in Appendix I, and a quick

⁵http://news.cnet.com/U.K.-banning-133-newsgroups/2100-1023_3-221558.html (last accessed 8 Dec 2014).

⁶Ibid.

review shows a list of content subjects relating to diverse sexual content and activity including illegal child abuse material. Some of the newsgroups referred to text newsgroups about homosexual activity, which was perfectly legal in the UK. It was a surprise at the time since newsgroups were diminishing in use, and usage of the World Wide Web was growing exponentially; there was real concern that causing Internet service providers liable for content on the Internet would have a major chilling effect on Internet adoption. It created a real debate in the Internet service provider industry about the possibilities for Internet blocking and Internet liability. It was known by both the Metropolitan police and the UK Internet service providers that users could still gain access to the full newsgroup list and content by accessing a newsgroup provider outside the UK based in a different European country or based outside Europe completely.

2.2.4 UK Child Pornography Laws [1]⁷

- In the UK, the Sexual Offences (Conspiracy & Incitement) Act 1996 became law in June 1996. Section 2 of the Act made it an offence to incite another person to commit certain sexual acts against children outside the UK. Section 2 extended the scope of incitement to ensure that any incitement by means of a telephone call, fax, Internet message or similar method is considered to have taken place in the UK if the message was received in the UK.
- The Protection of Children Act 1978 was passed in response to the growing problem of child pornography. Its main purpose was to close some potential gaps in the measures available to police and prosecutors. The definition of “photograph” given in Section 7(4) of the 1978 Act was extended to include photographs in electronic data format following the amendments made by Section 84 (4) of the Criminal Justice and Public Order Act 1994 (CJPOA 1994).
- The CJPOA 1994 introduced the concept of “pseudo-photographs” of children. Pseudo-photographs are technically photographs, but they are created by computer software manipulating one or more pre-existing pictures. For example, a child’s face can be superimposed on an adult body, or to another child’s body, with the characteristics of the body altered to create pornographic computer-generated images without the involvement of a real child. It is now an offence “for a person to take, or permit to be taken or to make, any indecent photographs or pseudo-photographs of a child; (or) to distribute or show such indecent photographs or pseudo-photographs” under Section 1 of the 1978 Act.⁸

⁷<http://www.cyber-rights.org/reports/governan.htm> (last accessed 7 Dec 2014). Akdeniz [1].

⁸Idem. (“*The UK police believed that the creators or possessors of pseudo-photographs would end up abusing children, so the purpose of the new legislation may be seen as to criminalise acts preparatory to abuse, and also to close possible future loopholes in the prosecution of such cases, as it may be very difficult to separate a pseudo-photograph from a real photograph.*”)

- As per Section 160 of the Criminal Justice Act 1988 Under Section 160 of the 1988 Act as amended by Section 84(4) of the CJPOA 1994, it is an offence for a person to have an indecent photograph or pseudo-photograph of a child in his possession. This offence is a serious arrestable offence with a maximum imprisonment term not exceeding 6 months.

Against this background, the European Commission produced a communication looking at the challenge of harmful and illegal Internet content.

2.2.5 The Protection of Minors and Human Dignity in Audio-Visual Services

The informal EC council meeting held in Bologna was followed by the informal meeting of Ministers of Justice and Home Affairs **on 26 and 27 September 1996** in Dublin during the 5th Irish Presidency of the European Union (EU), from July through December 1996, which discussed further cooperation between Member States to combat trade in human beings and sexual abuse of children.

On **23 October 1996**, the Commission produced a communication on “illegal and harmful content on the Internet” and a Green Paper on “the Protection of Minors and Human Dignity in Audio-Visual and Information services”. The Communication on Illegal and Harmful Content on the Internet, (Com (96) 487) in October 1996 and the Green Paper on the, Protection of Minors and Human Dignity in Audio-Visual and Information Services (Com (96) 483.) set the scene for all European initiatives in this area over the next decade from 1995 to 2005.

Two main types of preparatory work were carried out for the Green Paper. Firstly, the Member States were asked to reply to a questionnaire on the protection of minors and human dignity in the context of the development of services in the information society. All of the Member States responded favourably to this

(Footnote 8 continued)

Although pseudo-photographs can be created without the involvement of real children, there is a justifiable fear that harm to children is associated with all child pornography. The Williams Committee stated:

‘Few people would be prepared to take the risk Querywhere children are concerned and just as the law recognised that children should be protected against sexual behaviour which they are too young to properly consent to, it is almost universally agreed that this should apply to participation in pornography.’

On the other hand, there are arguments that pseudo-photographs are not harmful. The children involved in child pornography may suffer physical or mental injury, but with pseudo-photographs, the situation is quite different. These photographs are created only by the use of computers. There is no involvement of children in production and there is no direct harm to children in their use. However there is substantial evidence that photographs of children engaged in sexual activity are used as tools for the further molestation of other children, and photographs or pseudo-photographs will be used interchangeably for this purpose.”).

consultation processes. Secondly, with a view to the preparation of this Green Paper, the Commission commissioned a series of studies on the protection of minors and human dignity in the information society. These cover the regulatory, economic and technological aspects of the question in the 15 Member States, Canada, Japan and the USA. The Green Paper looked at the broader audio-visual services including radio, terrestrial and satellite television services and the Internet.

The Green Paper set out to examine the challenges that society faces in ensuring that two specific issues of overriding public interest, i.e. protection of minors and of human dignity, are adequately taken into account in the rapidly evolving world of audio-visual and information services. It was presented at the same time as the "Commission Communication on Illegal and harmful Content on Internet". The two documents were fully complementary, both as regards timing and scope. The fight against the dissemination of content offensive to human dignity and the protection of minors—against exposure to content that is harmful to their development—were considered of fundamental importance in enabling new audio-visual and information services to develop in a climate of trust and confidence. It underlined the need not to confuse problems that are different in nature, such as child pornography, which is illegal and subject to penal sanctions, and children accessing pornographic content for adults, which while being harmful for their development may not be illegal for adults. It points out that national arrangements in Europe are all set against the background of the fundamental rights enshrined in the European Convention of Human Rights (ECHR) which are incorporated in general principles of Community law by Article F.2 of the Treaty on European Union. In particular, Article 10 ECHR guarantees the right to freedom of expression. In the fight against illegal content, cooperation between the Member States in the field of justice and home affairs was identified as having a fundamental role to play given the international character of the new services. The potential for encouraging cooperation between the relevant industry sectors was also evaluated (codes of conduct, common standards for rating systems, promotion of PICS). Possible user awareness and media education measures are also put forward for debate.

The Green Paper identified a series of questions for further debate on issues the Commission considered important in order to define future policy actions. These included:

Question 1

Taking account of what is technically feasible and economically reasonable, what should be the liability of different operators in the content communication chain, from the content creator to the final user? What types of liability: penal, civil and editorial should come into play and under what conditions should liability be limited?

Question 2

How should the test of proportionality of any restrictive measures be applied? Inter alia, should any arbitration or conciliation mechanisms at European Union level be envisaged? If so, what sort of mechanisms?

Question 3

How do we determine the right balance between protection of privacy (including allowing users to maintain anonymity on the networks) and the need to enforce liability for illegal behaviour?

Question 4

Should one give priority to a regulatory or a self-regulatory approach (possibly backed up by legislation in the latter case) as regards parental control systems? What measures would be required, inter alia at the European Union level?

Question 5

In what cases should systematic supply of parental control systems be envisaged (according to service type or other criteria)? Should any obligatory regime be envisaged? If so, in what format and to which operators should it apply? What are the essential functions that such systems should provide?

Question 6

How can decentralisation of content rating be implemented, catering for the need to respect individual, local and national sensitivities, where audio-visual and information services are transnational?

Question 7

What elements of standardisation would allow content ratings to be developed in a coherent way in Europe, in particular in the case of digital services (standardisation of types of information to be supplied, of encoding and decoding of such information, etc.)?

Question 8

In what ways should administrative cooperation be implemented in the European Union? How and in what institutional framework should it be formalised?

Question 9

What should the priorities be at the European level and at the international level? In particular, should one give priority to developing solutions at the European Union level and then promoting them at the international level or should this be done in parallel? What are the most appropriate international fora for international cooperation (G7, DECD, ITU, WTD UN or bilateral relations)? How should this international cooperation be formalised?

In its communication from the Commission [2] to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on Illegal and harmful content on the Internet, the Commission recalls that illegal content relates to wider issues than child pornography.

- national security (instructions on bomb-making, illegal drug production and terrorist activities);
- protection of minors (abusive forms of marketing, violence and pornography);
- protection of human dignity (incitement to racial hatred or racial discrimination);
- economic security (fraud and instructions on pirating credit cards);
- information security (malicious hacking);
- protection of privacy (unauthorised communication of personal data and electronic harassment);
- protection of reputation (libel, unlawful comparative advertising); and
- intellectual property (unauthorised distribution of copyrighted works: for example, software or music).

The Internet was recognised as a symbol and had established itself as one of the main drivers of the convergence between telecommunications, computer and content industries. The Internet had also established itself as one of the main building blocks of the Global Information Infrastructure and as an essential enabler of the Information Society in Europe. Characterised by a growth rate unprecedented in the history of communication technologies, at the time of the Communication, the Internet had reached almost 60 million users in 160 countries and was doubling each year. The most popular application, the World Wide Web, based on protocols developed in Europe, was fast becoming a standard vehicle for information publication and electronic commerce, with an estimated 10 million sites worldwide in 1995, up 1600 % over the previous year.

As regards the distribution of illegal content on the Internet, it was clearly the responsibility of Member States to ensure the application of existing laws. What was illegal offline remains illegal online. Harmful content was defined as “both content which is allowed but whose distribution is restricted (adults only, for instance) and content which may offend certain users, although its publication is not restricted because of the principle of freedom of expression”. It is interesting to note that Internet issues were still considered as an extension of real-life crime and there was little attention given to new crimes facilitated by the Internet. It was also considered that the presence of illegal and harmful content on the Internet had “direct repercussions on the workings of the Internal Market. In particular, the adoption by Member States of regulations of new Internet services intended to protect the public interest may also create risks of distortions of competition (for example, through widely divergent responses to the question of potential liability of Internet service providers), hamper the free circulation of these services, and lead to a re-fragmentation of the Internal Market.”

A conference organised by the Association of London Government (“ALG”) called the First European Conference on Combating Violence and Pornography on the Internet was hosted on **13–14 February 1997** [3].⁹ The conference was organised to look at what could be done to combat violence and pornography on the

⁹http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz2/ (last accessed 7 Dec 2014).

Internet. The aim of the conference was to focus on the technical and moral issues around policing, legality and censorship to tackle the growing amount of and ever easier access to violence and pornography on the Internet. The conference aimed to influence European policy on tackling violence and pornography on the Internet. Mr. David Kerr stated that in December 1996, there were 28 reports from the online users which resulted in 5 pictures being removed from the UK ISP servers (mainly newsgroups). In January 1997, the Internet Watch Foundation had reported over 100 illegal items to the UK Police and there have been 50 additional reports by online users. Mr Kerr stated that most of the illegal contents on the Internet containing child pornography are posted from outside the UK and the EU (mainly from the USA) and international cooperation is needed to be effective.

According to a report written by Yaman Akdeniz¹⁰ about the conference, Mr. Jorg Tauss, a member of the German Bundestag Committee of Enquiry into Media and Violence, stated that he was against the policing of the Internet for pornography since it is widely available in the streets in his country. Mr. Tauss mentioned the difficulties in defining the word “pornography” and stated that this would be even more complicated in an international environment such as the Internet. While regulation of pornography would be difficult and unworkable, child pornography is a different issue. Mr. Tauss stated that the “Internet is not an illegal vacuum or beyond the rule of law” and that the police should take action to combat child pornography. Mr. Tauss also mentioned that the authorities do not understand the Internet at all and highlighted one case in Germany where the person who had reported child pornography to German authorities was himself prosecuted (because he had the material in his cache memory).

Whereas Sect. 1.3.1 noted that the whole development of the Internet was dominated by commercial interests and market forces and followed the principle of imposing no regulation for the sake of faster development, this was beginning to change. Rapid evolution of Internet services was still supported and encouraged, but it now needed to be supported by a self-regulatory, effective response to clearly articulated Internet concerns. In the early days, the concerns centred on bandwidth (spam and newsgroups) and on child protection, and sometimes these issues combined with the challenge of spam advertising child pornography websites.

Mr. David Kerr¹¹ was the first Chief Executive of the Internet Watch Foundation and company secretary, Internet Content Rating Association. He was appointed to the IWF in October 1996 to set up and run the organisation, and he was involved in developing public–private partnerships addressing issues such as race relations and rural services. He was appointed to IWF to implement an agreement between the UK Internet industry, government and the police. He was responsible for developing one of the world’s first hotlines for dealing with illegal net content with the support of the UK government, police and ISPs. He also played a leading role in specifying a UK rating system and in promoting the development of an

¹⁰Ibid.

¹¹<http://www.theguardian.com/technology/2000/apr/20/freespeech2> (last accessed 5 Dec 2014).

internationally acceptable rating and filtering scheme. He has led the INCORE project commissioned by the EU to make recommendations on the approach to rating and filtering from a European perspective, which is reporting in mid-2000. The ICRA, a not-for-profit consortium of global net players, was set up to deliver an international rating system. Later in 1999, he participated in the experts network set up by the Bertelsmann Foundation to consider issues of self-regulation of Internet content, which made recommendations to the Internet Content Summit in Munich in September 1999 and was jointly run by the INCORE.

UK ISPs were not present to discuss the availability of pornographic content on the Internet while their potential liability was discussed. Various ideas about self-regulation were discussed and the debate focused on the challenge of self-regulation and how self-regulatory solutions would operate and be effective (Internet Watch Foundation or rating systems such as PICS and RSACi). The main people concerned about the regulation of the Internet were non-users of the Internet.

On 17 February 1997, the council of the representatives of the governments of the member states [4] adopted a resolution on illegal and harmful content on the Internet (97/C 70/01) and stressed the importance of three action projects:

- encourage and facilitate self-regulatory systems including representative bodies for Internet service providers and users, effective codes of conduct and possibly hotline reporting mechanisms available to the public;
- encourage the provision to users of filtering mechanisms and the setting up of rating systems; for example the PICS (platform for Internet content selection) standard launched by the international World Wide Web consortium with Community support should be promoted;
- participate actively in the International Ministerial Conference to be hosted by Germany and encourage attendance by representatives of the actors concerned.

2.2.6 US Framework for Global Electronic Commerce

On 1 July 1997, the US government published a document on a Framework for Global Electronic Commerce (Clinton and Gore [5]).¹² President William J. Clinton and Vice President Albert Gore, Jr. wrote that “*the Internet is being used to reinvent government and reshape our lives and our communities in the process. As the Internet empowers citizens and democratizes societies, it is also changing classic business and economic paradigms. New models of commercial interaction are developing as businesses and consumers participate in the electronic marketplace and reap the resultant benefits. Entrepreneurs are able to start new businesses more easily, with smaller up-front investment requirements*”. They went on to say

¹²The Global Information Infrastructure (GII)—The Framework. <http://clinton4.nara.gov/WH/News/Commerce/read.html> (last accessed 8 Dec 2014).

that “Governments can have a profound effect on the growth of commerce on the Internet. By their actions, they can facilitate electronic trade or inhibit it”. Principles of the framework include the following:

1. The private sector should 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.
2. Governments should avoid undue restrictions on electronic commerce. Business models must evolve rapidly to keep pace with the breakneck speed of change in the technology; government attempts to regulate are likely to be outmoded by the time they are finally enacted.
3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce. Its goal should be to ensure competition, protect intellectual property and privacy, prevent fraud, foster transparency, support commercial transactions and facilitate dispute resolution.
4. Governments should recognise the unique qualities of the Internet. We should not assume, for example, that the regulatory frameworks established over the past sixty years for telecommunications, radio and television fit the Internet. Regulation should be imposed only as a necessary means to achieve an important goal on which there is a broad consensus. Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the needs of the new electronic age.
5. Electronic Commerce over the Internet should be facilitated on a global basis. The legal framework supporting commercial transactions on the Internet should be governed by consistent principles across state, national and international borders that lead to predictable results regardless of the jurisdiction in which a particular buyer or seller resides.

The framework identified that the goal was to ensure that online service providers can reach end-users on reasonable and non-discriminatory terms and condition, and there were several areas of concern such as access to leased lines, local loops pricing, interconnection and unbundling and attaching equipment to the network. Bilateral exchanges with individual foreign governments, regional fora such as APEC and CITEL, and multilateral fora such as the OECD and ITU, and various other fora (i.e. international alliances of private businesses, the International Organization of Standardization [ISO], the International Electrotechnical Commission [IEC]), also were used for international discussions on telecommunication-related Internet issues and removing trade barriers that inhibit the export of information technology. These issues include the terms and conditions governing the exchange of online traffic, addressing and reliability.

In the area of online content, four areas of concern were listed as follows:

1. Regulation of content,
2. Foreign content quotas,
3. Regulation of advertising,
4. Regulation to prevent fraud.

The Administration encouraged the creation of private fora to take the lead in areas requiring self-regulation such as privacy, content ratings and consumer protection and in areas such as standards development, commercial code and fostering interoperability.

It is clear that the focus of the US strategy was to encourage information society services and Internet growth, and there was very little consideration of the downside issues of the Internet such as emerging cybercrime trends. The conflict between responding to illegal and harmful content and supporting and encouraging Internet services became a major challenge in Europe.

Section 1.2 identified the problem of blurring boundaries which further contributed to the uncertainty as to who and how cybersecurity would be governed. It was not clear what the applicable legal and regulatory regimes were and which roles private stakeholders would play in safeguarding cyberspace. These framework papers, Green Papers and the European conferences started the debate to tease out the potential for safeguarding cyberspace and to identify the legitimate and reasonable roles of the variety of stakeholders. More importantly, it sought to identify the realistic limits of regulation, self-regulation and co-regulation in the new world of cyberspace.

2.2.7 Global Information Networks: Realising the Potential Conference, Bonn Germany

The Federal Republic of Germany and the European Commission jointly organised the European Ministerial Conference entitled “Global Information Networks: Realising the Potential”, held in Bonn from **6–8 July 1997** [6].¹³ Ministers from the Member States of the European Union, members of the European Free Trade Association and countries of the Central and Eastern Europe and Cyprus, members of the European Commission, guests from the USA, Canada, Japan and Russia and representatives from industry, users and European and international organisations attended the Conference. Ministers recognised the key role which the private sector is playing in the emergence of Global Information Networks, in particular through investments in infrastructures and services. They considered that the expansion of Global Information Networks must essentially be market-led and left to private

¹³http://web.mclink.it/MC8216/netmark/attach/bonn_en.htm#Heading01 (last accessed 7 Dec 2014).

initiative. They believe that private enterprise should drive the expansion of electronic commerce in Europe. Ministers also agreed that any regulatory framework for electronic commerce should be clear and predictable, pro-competitive, strike the right balance between the freedom of expression and the protection of private and public interests, in particular the protection of minors, and ensure consumer protection.

Ministers declared the emergence of Global Information Networks as a highly positive development. They considered this to be of crucial importance for Europe's future and an opportunity for all, businesses small and large, citizens and public administrations. They stressed the special characteristics and fundamentally transnational nature of the Internet which set it apart in almost every way from the then traditional means of communication. Ministers recognised that these new opportunities come with new challenges and that the sheer pace of development could have created technological and legal uncertainties. Such concerns, if not addressed, would delay investments by businesses and slow down take-up by users.

Ministers noted with satisfaction the key role taken by the industry itself in the process of standards setting. They considered that technological and commercial interoperability in a competitive environment was a vital factor for the development of Global Information Networks. Ministers recognised that it was crucial to build trust and confidence in Global Information Networks by ensuring that basic human rights were respected and by safeguarding the interests of society in general, including producers and consumers, particularly through fair and transparent offers of service. This could be achieved by protection of creativity and investment, security and confidentiality, digital signatures and responsibility of the actors.

The most important policy decision by Europe in the evolving area of self-regulation was made during this conference and the subsequent Ministerial declaration. Ministers stressed that the rules on responsibility for content should be based on a set of common principles so as to ensure a level playing field. Therefore, intermediaries such as network operators and access providers should, in general, not be responsible for content. This principle should be applied in such a way that intermediaries such as network operators and access providers are not subject to unreasonable, disproportionate or discriminatory rules. In any case, third-party content hosting services should not be expected to exercise prior control on the content which they have no reason to believe is illegal. Due account should be taken of whether such intermediaries had reasonable grounds to know and reasonable possibility to control the content. Ministers considered that rules on responsibility should give effect to the principle of freedom of speech, respect public and private interests and not impose disproportionate burdens on actors.

As noted in Chap. 1, when the government has no agenda for promoting and supporting self-regulation [...], the private sector itself can be very sceptical about self-regulation or initiatives may be undermined by state apathy towards lack of driving forces and uncertainty of, current legal statutes.

2.2.8 Irish Working Group on Illegal and Harmful Use of the Internet

In Dublin, in **March 1997**, I had a meeting with Mr. Colm Greely, well known for his time in Ireland Online (the first consumer-focused Internet service provider in Ireland). As a senior manager in Ireland Online and very knowledgeable on the Internet, he had been approached by the Irish Department of Justice, Equality and Law Reform about his participation on a committee assessing the impact of the Internet. He attended a few meetings and then decided he would approach me to determine if I would get involved with the project. We knew each other throughout my time in IEunet and respected the work we had both done. He explained to me that this new committee was created to investigate and make recommendations about the illegal and harmful use of the Internet. He was interested in the area, but his commitments to Ireland Online were significant, and more importantly, he was being asked to participate in the committee as an overall unbiased industry representative and not only as a representative of Ireland Online. Ireland Online was then working very closely with Postgem, which was a subsidiary of An Post and was in direct competition with Telecom Eireann. He described the individual participants in the committee on the illegal and harmful use of the Internet who were from a range of different sectors from Film Censorship, An Garda Siochana, Department of Enterprise and Employment, Department of Justice, Equality and Law Reform, Department of Foreign Affairs, Department of Finance, Department of Education, UNICEF, Department of Health and Children and Department of Communications, University College Cork, the University of Limerick and Ireland Online. For many of these participants, they had very basic knowledge of the Internet, how the Internet functioned, Internet services, Internet companies or stakeholders in the Irish market. The committee was chaired by Mr. John Haskins from the Department of Justice, Equality and Law Reform and was working through their terms of reference and developing a work plan for the committee meetings and the creation of targeted themed subgroups.

Colm suggested that I should take over his role as a broader industry representative in the committee since I knew most about the Internet services available in Ireland today and personally knew each of the Internet organisations, their management and many of their staff. I had managed to maintain their respect throughout my time in IEunet. He felt that it was too complex for him to represent the interests of his company while at the same time to represent the views of the wider Internet marketplace in Ireland. While he could make a reasonably fair attempt at achieving this balance, there was no forum for him to meet with competitors in the market and ask their views on a range of subjects in order to represent those views during meetings of the committee on illegal and harmful use of the Internet. Like Colm Greely, I could probably accurately estimate the views of the Internet service providers on a range of social, political and business issues, but I also understood that the open nature of this government committee meant it had the ability to move in a range of complex and diverse directions which would challenge the limits of my

experiences or knowledge. However, I would be able to meet with each of the industry players and could probably be accepted as a fair broker and representative of those views with no personal/professional agenda being in play. I therefore agreed to take on the role and started working on the committee from the next meeting.

The Working Group on Illegal and Harmful Use of the Internet [7] was created at a time when “the Internet still represents a vague concept to many people. Understandably, they find it difficult to grasp the idea of a network-of-networks-of-computers which has no central ownership, is almost indestructible and is growing at an unknowable rate”.

The terms of reference of the Working Group were guided by the European Commission that published a Green Paper on the Protection of Minors and Human Dignity in Audio-Visual and Information Services published on 16 October 1996. The terms of reference were to identify the nature and extent of the issues surrounding the illegal and harmful use of the Internet; to prioritise such issues with particular reference to the need to address the issue of child pornography in the short term; and to examine and assess the current approaches both domestically and internationally to addressing the problem of the illegal and harmful use of the Internet, in relation to those issues that can be domestically addressed, to identify the legal, technical and structural problems that arise; and to make specific recommendations for their resolution in the short, medium and long term as appropriate, in relation to those issues that require resolution in an international context, to make recommendations which will inform policy in this regard.

“In its mandate to examine the illegal and harmful use of the Internet, the Group was continually conscious of the need for balance in its treatment of the subject matter. The Internet allows the same ease of expression to evil as it does to good. In fact, it can be argued that with its relative anonymity and global dimensions, it facilitates the full expression of our darker side more than any other communication medium so far.” The inaugural meeting of the Group took place on 25 February 1997 and the deliberations of the Group extended over a period of 11 months. A total of 13 plenary sessions were held. Four subgroups covering Legal implications, International aspects, Child issues, and Issues relating to the role of Internet service providers (ISPs) also had several meetings, and 47 written submissions were received. The Group also heard a further 6 detailed oral presentations. Based on their particular experience in the area of combating child pornography on the Internet, Mr. David Kerr of Internet Watch Foundation (UK) and Mr. Nigel Williams of Childnet International were also invited to address the Group.

Mr. Nigel Williams¹⁴ (died 26 March 2006) was a native of Northern Ireland and the founder of the London-based charity Childnet International and had an international reputation for his work on the impact of the Internet on children. (In 2003, he was appointed as Northern Ireland’s first commissioner for children.) A significant part of his work with Childnet (established 1995), while working in

¹⁴<http://www.theguardian.com/society/2006/mar/31/childrensservices.northernireland> (last accessed 5 Dec 2014).

Westminster as head of public policy for Christian Action Research and Education (CARE), concerned pornography. He recognised the need to protect children from danger and published a book on the subject, *False Images*. Overall, however, he was clear that what information technology offered was essentially positive. Parents needed to recognise that their children would benefit from what he called this “parallel universe”. He was also a board member of the Internet Watch Foundation and the Internet Content Rating Association, and in 2001, it was appointed to the home secretary’s task force on child protection on the Internet.

The period from 1996 to 1998 was an amazing period in the evolution of self-regulation. The methodology adopted offered a focused structured process to identify the essential issues relating to Internet technologies and the diverse services evolving from their widespread adoption. A number of the working group members were quite knowledgeable on the subject area, but there were also quite a few who had very limited understanding of the operation of the Internet, the range of different organisations responsible for effective Internet operation and the different levels of knowledge and capabilities of these organisations in any effective self-regulatory response. In addition, the range of illegal activities and harmful activities possible was identified and the difference between current criminal activities in the real world and online crime was debated. It was a very thought provoking process. These areas are highlighted in Fig. 2.1.

As an Internet technology expert, I was respected by all members of the working group. As a person representing the interests of the wider Internet industry, my opinion was treated with suspicion and assumed to be focused on the short-term

<p>National security:</p> <ul style="list-style-type: none"> • Terrorist activities • Instructions on bomb making • Hacking into government computer networks <p>Injury to children</p> <ul style="list-style-type: none"> • Child pornography • Adult pornography • Material depicting extreme violence • Child trafficking • Advice on anonymous exchange of graphic material <p>Injury to human dignity</p> <ul style="list-style-type: none"> • Racial discrimination, incitement to racial hatred • Extreme sexual perversion <p>Economic security</p> <ul style="list-style-type: none"> • All types of fraud • Instructions on credit card piracy 	<p>Information security</p> <ul style="list-style-type: none"> • Malicious hacking <p>Privacy protection</p> <ul style="list-style-type: none"> • Unauthorised mailing • Interception of personal e-mail • Misuse of personal data • Unfair obtaining of personal data <p>Protection of reputation</p> <ul style="list-style-type: none"> • Libel <p>Gambling</p> <p>Information on or sale of “controlled drugs”</p> <p>Intellectual property</p> <ul style="list-style-type: none"> • Copyright infringements of any medium • Unauthorised distribution of videos, music, software etc.
--	---

Fig. 2.1 1998 Sect. 1.3.1 First Report of Illegal and Harmful use of the Internet—the concept of illegal use of the Internet covers a wide range of subject matter under a diverse range of identified categories

narrow interests of the industry. It was a challenging period to share my knowledge of Internet systems and the low level of cooperation and sharing between the different industry players. Whereas the early interests of the working group were to understand the detailed inner workings of networked computer systems and the Internet in particular, the emphasis on gaining a deeper understanding on the range of Internet services, protocols and the international nature of Internet activities was of immense importance. At times, it seemed that the range of issues would overwhelm the aims and objectives of the committee.

To support this process, documents were prepared describing the structure of the industry and the layers of interconnectivity at the organisational level. These documents described the level of visibility these players had at different levels in the technology network models. It is necessary to understand the various players in the industry and their role in relation to the carrying, processing and storage of information on its journey throughout the Internet. The roles can be broken into seven main areas including the consumer groups (Individuals, Families, companies, Research Organisations, Universities, Schools, Government Agencies, Employees, Students, etc.), the telecommunications circuit provider, the Internet access provider (including TCP/IP address allocation, domain name registration, dial-in facilities, email, newsgroup and the web services), the facilities providers (include hosting and web farm), the content providers, the broadcasters and the regulatory agencies. For example, the role of a Domain Registry both at the country level and at the global level was described in detail. Prepared documents described the different Internet services being sold, how they are implemented and the possibilities of interception and disruption of illegal and harmful activities. Section 1.5.3 of the proposed NIS directive [8] indicates out these categories have continued to increase including a greater number of industry stakeholders including e-commerce platforms, Internet Payment gateways, social networks, cloud computing services and application stores. These were later increased to include Internet exchange points, national domain name registries and the web hosting services.

An alternative method of describing the roles is to do so in terms of the electronic services provided including electronic mail, network news, web browsing, web provision, online chat, file transfer and other services. (Note that Social Networking Services had not started operating yet.) I described the potential options the different stakeholders could implement in combating illegal and harmful content. The data travelling across the ISP network operations centre (backbone) are processed automatically and unless deliberately intercepted are never seen, heard or read by human operators. The sheer volume and complexity negated any reasonable analysis without prior knowledge and specific targeting of potential abuse.

2.2.9 Electronic Mail

Email allows the exchange of messages and documents in a one-to-one and one-to-many manner. These messages are usually plain text, but attached files can be

graphics, spreadsheets, reports, etc. It is also possible to encrypt email content to prevent others from intercepting it. Email can be particularly difficult to regulate since the messages can be considered as communication between parties with entitlements to privacy and confidentiality. The communication can be encrypted preventing interception and therefore regulation. One aspect of email activity which can be regulated is that of “spamming”—a process where volume email is targeted at end-users without their request—in essence “junk” mail.

2.2.10 Newsgroups

The newsgroups are spread across 15,000 different topics, and in theory, it is possible to prevent the distribution of specific newsgroups. However, there is no technical method of controlling the content of any newsgroup—it is subject to self-regulation and net etiquette. The blocking of specific newsgroups is feasible but cannot be considered as a definitive solution to illegal or harmful content. It is possible for users to inject news messages into the news system using international news hosts, thus bypassing local regulations. In addition, users can read the news database stored on international servers which would have a significant impact on international bandwidth if large numbers were to adopt this approach.

2.2.11 Web Browsing

Web browsing allowed end-users to use Microsoft Internet Explorer¹⁵ or Netscape Navigator¹⁶ from Netscape to browse information in a graphical and hierarchical manner on remote servers located in all countries of the world. This content could span the full range of work-related research material, edutainment for home education to illegal and harmful material. The wide range of dubious material has created real concerns among many Internet users. Its success continues to grow and newer technologies will enable faster and wider distribution of the web content. The recent standards in relation to PICS¹⁷ (Platform for Internet Content Selection) allow substantial choice in the categorisation of website content. Browsing software now checks each site selected for a site rating hosted on a separate server for the style and content of the selected site. Simple rules can permit or deny access to sites

¹⁵Microsoft originally released Internet Explorer 1.0 in August 1995.

¹⁶Netscape Navigator 1.0 initial release was on 15 December 1994.

¹⁷<http://www.w3.org/PICS/> (last accessed 8 Dec 2014). The PICS specification enables labels (metadata) to be associated with Internet content. It was originally designed to help parents and teachers control what children access on the Internet, but it also facilitates other uses for labels, including code signing and privacy. The PICS platform is one on which other rating services and filtering software have been built. PICS has been superseded by the Protocol for Web Description Resources (POWDER).

based on criteria specified by the parent, manager or users themselves. In addition, end-users and institutions would want rating agencies particularly tuned to their ethos and responsibilities.

2.2.12 Web Hosting

Websites could be hosted anywhere in the world, and a single site can even span multi-jurisdictional boundaries. The site can contain text, graphics, video clips, music and sound clips in addition to more complex interfaces to remote databases which can be located in different geographical boundaries.

2.2.13 File Transfer

File transfer permitted the copying of documents, graphics, video clips and audio clips from any part of the world onto the local computer or from the local computer onto a remote computer system. The file transfer process was normally performed manually by the user, but on many systems could be completely automated. The remote files could be encoded, compressed and even encrypted. Many systems offered anonymous FTP facilities which were essentially a large volume of publicly accessible files available for download by anyone without password access. Some organisations offer controlled (username and password) access to files and documents for a financial charge.

2.2.14 Online Chat

CHAT (not to be mistaken with Voice-over IP—voip which arrived later) was the Internet equivalent of voice chat lines except that the users participating in the forums each type their message which is then copied onto the screen of each participant in the group. The “conversations” could cover a very broad range of subjects including illegal and harmful areas. Many of these discussion groups were publicly advertised and users could specify to their chat software that they are interested in taking part. It is also possible to have closed group discussions by prior arrangement. The primary target of any regulatory activity would be the publicly advertised groups. This would still be a major technical problem since the location of the broadcast point can easily move across international boundaries with ease.

There were several major issues identified which are critical to any conversation or debate on self-regulation. Firstly, there was the issue of the critical and important difference between illegal and harmful content and activity. The report stated that “decisions on acceptability of harmful material are subjective and are very much

context-based. There are variations in levels of acceptability not only between countries but also within countries. What some people might find distasteful and offensive, others may not. While the cultural norms may mediate what is considered to be ‘acceptable’, any form of consensus is, at best, problematic”.¹⁸

The second issue was the recognition that there are significant differences in any effective response to activity- and content-related issues (illegal or harmful).

The third critical issue was the acceptance that the Internet was international in nature and that it would be technically challenging for any single country to adopt and implement a national approach to Internet issues which was not internationally accepted and endorsed. It required international collaboration to be effective.

Much of the work of this group is still relevant today, and although many of the risks identified in this working group have received much attention and disruption as a result of a range of international effective responses, a number of challenges listed in this report remain unresolved. The pace of change on the Internet continues to be phenomenal.

Much of this research was performed *before* Web 2.0 and before social networking services, peer-to-peer software solutions, voice-over-IP (voip) and mobile Internet services were adopted widely. In addition, most users were accessing the Internet over slow-speed links.

2.2.15 Child Pornography

The Irish working group gained a real insight into current research on child pornography on the Internet and the state-of-the-art research being conducted by Prof Max Taylor and Dr. Ethel Quayle in University College Cork. They were researching the increasing production and distribution of child pornographic images on the Internet and created a methodology to grade the type of images into different categories. This work was internationally recognised and created increased awareness and understanding of the increasing risks associated with online crime activity in this area.

2.2.16 Recommendations of the Committee on Illegal and Harmful Use of the Internet

- Self-regulation: A system of self-regulation by the service provider industry should be introduced to include common codes of practice and common acceptable usage conditions.

¹⁸http://www.justice.ie/en/JELR/Pages/Illegal_use_of_the_Internet_report Page 15 (last accessed Dec 14).

- **Complaints hotline:** A non-statutory national complaints hotline should be established to investigate and process complaints about illegal material on the Internet.
- **Advisory Board:** A non-statutory advisory board representative of the significant players involved should be established to oversee and coordinate measures aimed at ensuring the success of the self-regulatory framework.
- **Awareness:** Any national awareness campaigns proposed by the Information Society Commission should include a dimension which addresses the potential for illegal and harmful use of the Internet.
- **Other awareness measures should include:**
 - An active role for service providers in the education of their clients on the safe use of the Internet.
 - The active involvement of the new hotline and Advisory Group in the development of awareness programmes.
 - The specific targeting of parents and teachers.
 - The incorporation of modules on Internet safety into the curriculum of teachers, care workers, Gardaí, Customs officers and any other agencies who come in contact with issues relating to the downside of the Internet.
- **Specific initiatives for schools should include the following:**
 - In-career training modules for teachers on Internet issues.
 - The publication of a set of guidelines by the Department of Education and Science for those involved in the Internet in schools.
 - The integration of Internet Ethics into the Curriculum.
 - The staging of information sessions for Parents/Guardians.
 - The development of a Schools Code of Conduct.
- **Funding:** The initial funding of the hotline should be shared by Government and the service provider industry. The service provider industry should immediately and actively pursue EU funding opportunities which are now available in the area of Internet safety.
- **Legislation:** New legislation and any reviews of existing legislation should be “Internet proofed” before being submitted to Government for approval.
- **Specialist training:** Specialist training programmes already begun in the policing area should be urgently pursued and extended to the wider areas of law-enforcement including the judiciary.

2.2.17 Internet Service Provider Associations

A key challenge in the self-regulation area was to have a platform to communicate with the Internet industry. The formation of the ISP associations across Europe and the subsequent representation of the ISP view at government events to promote the

views, concerns and interests of the Internet service provider was a critical step forward. The continued development of the ISP associations across Europe and the degree to which they represented the interests and combined energy and resources of all providers was critical to the successful implementation of self-regulation. This was a period of much market upheaval and the composition and ownership of the Internet service providers went through significant change during these years; this continued to evolve as the Internet market developed.

EuroISPA¹⁹ is a pan-European association of European Internet Services Providers Associations (ISPAs). It is the world's largest association of Internet service providers (ISPs), representing over 2300 ISPs across the EU and EFTA countries—including ISPs from Austria, Belgium, the Czech Republic, Finland, France, Germany, Ireland, Italy, Norway, Romania and the UK. The association was established in 1997 to represent the European ISP industry on EU policy and legislative issues and to facilitate the exchange of best practices between national ISP associations. Its secretariat is located in Brussels. EuroISPA is recognised as the voice of the EU ISP industry and is the largest “umbrella” association of Internet service providers in the world. The reason for EuroISPA reflects the views of ISPs of all sizes from across its member base. EuroISPA has signed Memoranda of Understanding with the following organisations: APIA—Asia & Pacific Internet Association; APJII—Indonesian Internet Service Provider Association; CAIP—Canadian Association of Internet Providers; CENTR—Council of European National Top Level Domain Registries; ECOMLAC—Latin America and Caribbean Federation for Internet and Electronic Commerce; HKISPA—Hong Kong Internet Service Providers Association; IIA—Australian Internet Industry Association; INHOPE—The Association of Internet Hotline Providers in Europe; ISPA SA—Internet Service Providers Association South Africa; TELESAs—Telecom Services Association, Japan; and US ISPA—United States Internet Service Provider Association.

ECO²⁰—The Association of the German Internet Industry, was founded in 1995, has almost 800 member organisations and is the largest Internet industry association in Europe. ECO has been instrumental in the development of the Internet in Germany, fostering new technologies, infrastructures and markets, and forming framework conditions. One of the most important tasks is to represent the interests of ECO members in politics, and in national and international committees. ECO is a member of EuroISPA.

The UK Internet Service Providers' Association (ISPA)²¹ was established on 8 August 1997 and is the UK's Trade Association for providers of Internet services. ISPA promotes collaboration and constructive dialogue between its members and the wider Internet community. Companies who choose to become members of ISPA agree to abide by the ISPA UK Code of Practice which was adopted on 25

¹⁹www.euroispa.org (last accessed 8 December 2014).

²⁰<https://international.eco.de/about.html> (last accessed 8 Dec 2014).

²¹<http://www.ispa.org.uk/about-us/ispas-industry-role/> (last accessed on 8 Dec 2014).

January 1999. Allegiance to the code means that consumers can view the ISPA UK logo as a mark of commitment to good business practice. ISPA UK was instrumental in founding the Internet Watch Foundation, the UK hotline for reporting illegal online content in 1997 and holds permanent membership. As one of the many funding organisations of the IWF, along with many other ISPA members, ISPA sits on the funding council. The success of the IWF and self-regulation has seen the amount of child abuse images hosted in the UK fall from 18 % in 1997 to less than 0.1 %.

The main Irish service providers formed the Internet Service Providers Association of Ireland (ISPAI) in April 1997. On 5 May 1998, the Internet Service Providers' Association of Ireland²² was formally registered as a not-for-profit company limited by guarantee of its members, under Company Number 285632. The Association provides one voice for the Irish ISP Industry at the National, International and EU levels. The ISPAI, among other responsibilities, maintains a Code of Practice and Ethics recognised as a role model in the EU and operates a fully functioning and efficient Internet Hotline Service. ISPs agree to adhere to the Code of Practice and Ethics when they become members of the ISPAI.

2.2.18 Bertelsmann Foundation

In **September 1999**, the Bertelsmann Foundation project “Self-Regulation of Internet Content” (Bertelsmann 1999) produced a report which dealt with the problem of harmful and illegal content and the protection of minors on the Internet. Starting from the assumption that no nation state, no major Internet industry player, nor any law enforcement authority could handle this complex task on its own, the project took a coordinated approach in four areas:

- Self-regulation and the Internet industry
 - Only such a systematic approach—bringing technological potential together with the energies and capacities of government, the Internet industry and the citizenry—has the promise of success in meeting what often seem to be competing goals.
 - As part of the codes of conduct, Internet providers hosting content have an obligation to remove illegal content when put on notice that such content exists. The procedure for such notice and takedown—while laid down by regulation—should be reflected in codes of conduct and should specify the requirements for proper notification of service providers.
- Self-rating and filtering
- Hotlines as a feedback mechanism for users
- Law enforcement and the role of legal provisions in supporting self-regulation.

²²<http://www.ispai.ie/about/> (last accessed 8 Dec 2014).

It offered 12 recommendations:

- The Internet: changing the way people live
- Self-regulation of Internet content: towards a systematic, integrated and international approach
- Internet industry: developing and implementing codes of conduct
- Sharing responsibility: self-regulatory agencies enforcing codes of conduct
- Governments: supporting and reinforcing self-regulation
- Self-rating and filtering systems: empowering user choice
- Internet filtering: ensuring youth protection and freedom of speech
- Hotlines: communicating and evaluating content concerns
- International cooperation: acting against content where it is located
- The legal framework: limitations on liability
- Law enforcement: cooperation and continuous training
- A “learning system”: education and constant evaluation.

2.2.19 EC Daphne Programme

The INHOPE Forum was established in 1998 with financial assistance from the 1997 Daphne Programme,²³ to bring together hotline initiatives across Europe which were responding to child pornography on the Internet. Hotlines provided an easy point of contact and reporting mechanism for Internet users who come across child pornography. Hotlines evaluated these reports according to their procedures and national legislation, and then link with industry and/or the police to ensure the material was removed and/or subject to enforcement action. The 1997 Daphne project had enabled Internet hotlines to come together for the first time and discuss issues of common concern in a very fast-moving environment. This project was undertaken by Childnet International in conjunction with the members of the INHOPE Forum including Austria—ISPA, Finland—Mannerheim League for Child Welfare, France—AFA, Germany—Eco-Forum; FSM; and Jugendschutz.net, Ireland—ISPA Ireland and Norway—Redd Barne. It was supported by the National Center for Missing and Exploited Children in the USA.

In 1999, there were three international conferences that addressed the issue of child pornography on the Internet which are listed below:

- the UNESCO conference in Paris in 18–19 January 1999 was a meeting of experts entitled Sexual Abuse of Children, Child Pornography and Paedophilia on the Internet: an International Challenge [9]. In the framework of the United Nations Convention on the Rights of the Child, this initiative aimed to “alert world opinion to the need to fight child pornography, to combat sexual abuse of

²³http://ec.europa.eu/justice_home/daphnetoolkit/html/projects/dpt_1998_045_c_en.html (last accessed 8 Dec 2014).

children resulting from the misuse of the Internet, and the mobilisation of human, technical and financial resources to support the work of professionals and non-governmental organisations in the protection of children and to safeguard their rights in the media and on the Internet”; UNESCO created a website called INNOCENCE IN DANGER²⁴ and convened a conference, involving over 300 delegates, to discuss

- The sexual abuse of children: family, social and economic context: origins, causes, prevention and care;
 - Combating sexual abuse of children: role of civil society;
 - Legal and judicial aspects; crime detection and law enforcement: crime detection and law enforcement, extradition;
 - Promoting the free flow of information in the face of worldwide concern about the sexual abuse of children, child pornography and paedophilia on the Internet;
 - Civil liberties, privacy and Internet abusers; making the Net safe for young children—content providers, spam filters, search engines, self-rating of websites, monitoring and networking;
 - Research, information and monitoring sensitisation of the public.
- the Bertelsmann Foundation conference in Munich in September 1999 also addressed wider issues of Internet content and Internet rating. The results of this conference are outlined in the previous section.
 - the International Conference on Combatting Child Pornography on the Internet was jointly sponsored by the EU, US Government and Austrian Government on 29 September to 1 October 1999. It was organised by Austrian Foreign Minister Wolfgang Schuessel and US Secretary of State Madeleine Albright and supported by the European Union. The conference intended to mobilise public opinion and encourage cooperation and coordination between judicial and industry authorities. Senior representatives from European and US justice and interior ministries participated with others from the United Nations, the European Commission, non-governmental organisations and Internet companies. A network of child pornography operating on the Internet was broken up in August in Vienna and Linz, central Austria, as police arrested three people, including a Catholic priest.²⁵ The objectives of the conference were to reinforce cooperation among law enforcement officials and the judiciary; to re-establish voluntary self-regulatory mechanisms (codes of conduct) among Internet service providers; and to encourage the establishment of further hotlines (hotlines enable citizens to report leads on child pornography found on the Internet) and of networking among existing hotlines.

The work of the INHOPE Forum complemented these large events by bringing together the specialist group of hotlines dealing with child pornography on the

²⁴<http://www.unesco.org/bpi/eng/unescopress/1999/99-219e.shtml> (last accessed 9 Dec 2014).

²⁵<http://www.cyber-rights.org/reports/interdev.htm> (last accessed 9 Dec 2014).

Internet on a day-to-day basis. The work of the INHOPE Forum and the three conferences in 1999 were the foundation of the EC Safer Internet Action Plan. This was also the beginning of the link between child protection issues as an inherent element of Internet self-regulation.

2.2.20 EC Safer Internet Action Plan

On 26 November 1997, a Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions Action Plan on promoting safe use of the Internet proposal for a council decision adopting a Multiannual Community Action Plan on promoting safe use of the Internet was proposed. The action plan proposed in the communication was described as an important element to combat illegal and harmful content on the Internet. To be effective, it would be closely coordinated with other initiatives in the area of illegal and harmful content, and it would build a bridge to the growing cooperation between police and judicial authorities under the third pillar.

The intense activity of the European institutions in this area since 1996, the political direction given by the European Parliament² and the Council, the Ministerial Declaration resulting from the Bonn Conference and the developments in Member States demonstrated that Europe had in many respects been a pioneer in addressing the issues and proposing solutions based on industry self-regulation, filtering and rating, and increasing user confidence through awareness.

The Commission identified areas where concrete measures are needed and where community resources should be made available in order to encourage an environment favourable to the development of the Internet industry:

- promotion of self-regulation and creation of content-monitoring schemes including an European network of hotlines to achieve a high level of protection (especially dealing with content such as child pornography, racism or anti-semitism);
- demonstration and application of effective filtering services and compatible rating systems, which take account of cultural and linguistic diversity; and
- promotion of awareness actions directed at users, in particular children, parents and teachers, to allow them to use Internet resources provided by industry safely and with confidence.

It took two more years for the Commission Communication to become Decision No 276/1999/EC [10] when on 25 January 1999, the European Parliament and of the Council adopted a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. It acknowledged that cooperation from the industry in setting up voluntary systems of self-regulation can efficiently help to limit the flow of illegal content on the Internet. The action plan covered the period of four years from 1 January 1999 to 31 December 2002, and the financial framework for the implementation of the plan

was set at €25 million. The action plan was later extended [11] until 31 December 2004, and the budget increased by €13.3 million to cover the two extra years.

In summary, it clarified that the distinction between illegal and harmful content is important²⁶ as these two types of content are dealt with differently:

- illegal content must be dealt with at source by the police and the judicial authorities, whose activities are covered by national legislation and judicial cooperation agreements. However, the industry can be of considerable assistance in restricting the circulation of illegal content (particularly in the case of child pornography, racism and anti-semitism) by means of effective self-regulation schemes (such as codes of conduct and hotlines) governed and supported by legislation, and with consumer backing;
- harmful content is both that which is authorised but has restricted circulation (e.g. for adults only) and content which could be offensive to some users, even if publication is not restricted because of the freedom of speech. Action to combat harmful content first and foremost means developing technology (filtering tools and rating mechanisms) to enable users to reject such content by promoting awareness among parents and fostering self-regulation, which could be an adequate way of protecting minors in particular.

The action plan is divided into four sections:

- establishing a safer environment through a European network of “hotlines” and by encouraging self-regulation and the adoption of codes of conduct;
- developing filtering and rating systems, in particular by highlighting their benefits and facilitating an international agreement on rating systems;
- encouraging awareness campaigns at all levels to inform parents and all people dealing with children (teachers, social workers, etc.) of the best way to protect minors against exposure to content that could be harmful to their development; and
- conducting support activities to assess legal implications, providing coordination with similar international initiatives and assessing the impact of community measures.

On 3 November 2003, there was a Communication from the Commission concerning the evaluation of the Multiannual Community Action Plan [12] on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors. The report stressed the positive impact of the action plan, particularly in fostering networking and providing a wealth of information about the problems of safer use of the Internet. In particular, the report concluded that:

- the programme had achieved a good result in producing a number of filtering software products although take-up of rating needed to be increased. Moreover, not all stakeholders agreed that filtering was the best approach to child

²⁶http://europa.eu/legislation_summaries/information_society/Internet/I24190_en.htm (last accessed 8 Dec 2014).

protection. At the policy level, the programme was successful in putting the issues of developing a safer Internet firmly on the agenda of the EU and the Member States;

- at action-line level, the Commission had instigated the development of a network of hotlines in Europe with associated members in the USA and Australia, funded research into tackling awareness-raising with end-users, stimulated the development of filtering and supported the development of an international rating system; and
- the programme had been successful in linking up stakeholders to produce a “community of actors”, although the commission is disappointed by the lack of industry involvement as well as self-regulation organisations and consumer groups.

On 11 May 2005, the Council adopted a Decision establishing the Safer Internet Plus programme [13], to cover the years 2005–2008, aimed at promoting safer use of the Internet and new online technologies. A budget of €45 million was allocated to the programme for the period 2005–2008, and almost 50 % of the budget was allocated for awareness-raising measures. The new programme was geared towards the following activities:

- funding hotlines, so that they could act at national level and cooperate with other centres in the European network of hotlines;
- supporting telephone helplines for children confronted with illegal and harmful content;
- collection of qualitative and quantitative data on the establishment and operation of hotlines;
- launching incentive measures to speed up the process of setting up hotlines and developing codes of conduct; and
- setting up a coordination centre for the network to raise its visibility at European level, improve its operational effectiveness and promote exchanges of information and experience.

The programme provided funding for technological measures which enable users to limit the amount of unwanted and harmful contents and manage the spam they receive. This included:

- assessing the effectiveness of available filtering technology;
- facilitating and coordinating exchanges of information and best practices;
- increasing take-up of content rating and quality-site labels; and
- if necessary, contributing to the accessibility of filter technology, notably in languages not adequately covered by the market.

A fully functioning system of self-regulation was considered to be an essential element in limiting the flow of unwanted, harmful and illegal content. It was considered that self-regulation involved a number of components: consultation and appropriate representation of the parties concerned, codes of conduct, national bodies facilitating cooperation at Community level and national evaluation of self-regulation frameworks. To improve self-regulation in the sector, the Commission

provided national co-regulatory or self-regulatory bodies with the Safer Internet Forum as a platform for exchanging experience. The Forum was set up in 2004 under the Safer Internet Action Plan. Its objectives were given as follows:

- to stimulate networking of the appropriate structures within Member States and developing links with self-regulatory bodies outside Europe;
- to stimulate self-regulation on issues such as quality rating of websites, cross-media content rating, rating and filtering techniques, extending them to new forms of content such as online games and new forms of access such as mobile phones;
- to encourage service providers to draw up codes of conduct; and
- to promote research into the effectiveness of rating projects and filtering technologies.

On 5 May 2012, a Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions described a European Strategy for a Better Internet for Children. It stated that children have particular needs and vulnerabilities on the Internet, which must be addressed specifically so that the Internet becomes a place of opportunities for children to access knowledge, to communicate, to develop their skills and to improve their job perspectives and employability [14]. The strategy²⁷ proposed a series of actions grouped around the following main goals:

- stimulate the production of creative and educational online content for children as well as promoting positive online experiences for young children;
- scaling up awareness and empowerment including teaching of digital literacy and online safety in all EU schools;
- create a safe environment for children through age-appropriate privacy settings, wider use of parental controls and age rating and content classification; and
- combat child sexual abuse material online and child sexual exploitation.

2.2.21 The INHOPE (Internet Hotline Providers of Europe) Association

During 1995–1999, various national initiatives brought together the relevant stakeholders to consider how to prevent illegal activity and especially the abuse of children on the Internet. These initiatives were briefly mentioned in Sect. 1.3 which lists the early hotline initiatives.

In Germany, a number of separate initiatives commenced that were first discussed at the time of high-profile court cases and parliamentary debates in 1995/1996. In June 1996, the first Internet child pornography hotline was established in the Netherlands by concerned individuals in the industry and among users, with the

²⁷Key priorities of the EU e-Skills strategy “e-Skills for the twenty-first century” COM(2007)496.

support of the police. This was quickly followed by initiatives in Norway, Belgium and the UK before the end of 1996. Other countries began to take notice, and plans for hotlines were being finalised in Austria, Ireland, Finland, Spain and France. The issue was extensively debated in other European countries as well. In March 1998, the USA launched its “Cybertipline” which quickly became established as one of the busiest hotlines.

In 1997, the INHOPE Forum was created and 8 hotlines came together to form the INHOPE Association. The hotlines agreed the statutes of the association, and it was formally established as a Dutch company on 23 November 1999. The first executive was elected on that date, and Ms. Ruth Dixon, Assistant Chief Executive of the United Kingdom Internet Watch Foundation, was elected as inaugural President. The organisation continues today and meets regularly to share and exchange knowledge and best practices in the operation of Internet hotlines.

Hotlines must provide a mechanism for receiving complaints from the public about alleged illegal content and/or use of the Internet; they must have effective transparent procedures for dealing with complaints, and they must have the support of government, industry, law enforcement and Internet users in the countries of operation. In addition to these requirements, to be a member of INHOPE, a hotline must cooperate with other members in exchanging information about illegal content, share their expertise, make a commitment to maintain confidentiality and respect the procedures of other members. The purpose of a hotline is to quickly and efficiently remove illegal material from the Internet, to enable a swift investigation by Law Enforcement and to collaborate at the international level with other members of INHOPE.

Each hotline has a strong mandate from the appropriate National Government, Internet Industry, Law Enforcement and Child Welfare. This broad support has been essential to the success achieved so far. There have been many lessons learned during the last two years that were extremely demanding on INHOPE and the individual hotlines. Even though each country has its own individual legislation relating to illegal material on the Internet, the primary focus of the INHOPE association relates to illegal child pornography and online abuse of children. However, some hotlines also deal with illegal adult pornography and/or crimes of xenophobia and racism.

2.2.22 Legislation and Conventions

From the year 2000 onwards, the focus shifted towards regulatory activities with self-regulation evolving towards a multi-stakeholder, co-regulated approach. The Internet industry players were strongly encouraged and motivated through the carrot and stick approach of reasonable legislation supported by threats of draconian regulations in order to continue to support self-regulatory activities. This was very much supported by industry stakeholders who preferred to maintain direct control over their organisations and their ethical stance based on market pressure and customer demands while enabling dynamic business ideas and models to be tested on the Internet.

During the period from 2000 to 2010, there was significant growth of new legislation. In Europe, the focus was on regulation of electronic commerce, online copyright protection, child protection, data protection, data retention and critical infrastructure protection. All these areas required significant participation and commitments from Internet Industry and were set against the background of continually evolving Internet technologies and the global impact of mobile technologies and the arrival of the computer touch screen tablet. This was also the period when social networking and Internet 2.0 later arrived into the mainstream.

2.2.23 Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce

There are two documents of Interest which were significant milestones in the support and encouragement of the Internet industry self-regulation: firstly, directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 titled on certain legal aspects of information society services, in particular electronic commerce [15] and was one of the cornerstones of self-regulation. Section 2.4 of this directive clearly specified the liability of intermediary service providers through the definition of “mere conduit” for Internet society services, article 13 with the definition of “caching”, article 14 with the role of hosting providers and article 15 with the prohibition of a general obligation of monitoring services. These articles were the most important legal specifications in the European sphere to describe the role, responsibilities and limitations of Internet service providers. Article 13 clearly states that the “*service provider is not liable for the information transmitted, on condition that the provider [...] does not select or modify the information contained in the transmission.*” This is explicitly refined in Article 14 that “*Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information*”. Article 16 describes the role of codes of conduct.

2.2.24 The Council of Europe Cybercrime Convention

On 23 November 2001, the Council of Europe Cybercrime convention [16] was opened for signature by the Member States of the Council of Europe and by non-Member States that have participated in its elaboration, in Budapest. It entered into

force on 1 July 2004. In November 1996, the European Committee on Crime Problems (CDPC) decided (CDPC/103/211196) to set up a committee of experts to deal with cybercrime. On 4 February 1997 (at the 583rd meeting of the Ministers' Deputies), the Committee of Ministers set up the new committee, called "the Committee of Experts on Crime in Cyber-space (PC-CY)". This Committee PC-CY started its work in April 1997 and undertook negotiations on a draft international convention on cybercrime. Although, under its original terms of reference, the Committee was due to finish its work by 31 December 1999, the document was not completed until December 2000. The text of the convention was developed over the previous years and succinctly specified the challenges of cybercrime and described the preferred roles and responsibilities of the Internet service providers in combating cybercrime. It serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between State Parties to the treaty. The convention was the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. For industry stakeholders, the convention created definitions for issues and activities which were in constant debate but rarely agreed and enabled a precise and simple debate to occur in relation to international collaboration on cybercrime issues. In particular, it provided the first internationally agreed definitions on types of crime. It further enabled the debate on traffic data as a separate entity than the content of data communications, which were subject to stricter data protection rules. This later evolved into discussions on traffic meta-data which became subject to data retention and data disclosure legislation and is still debated intensely today. It created understandings on expedited preservation and expedited disclosure including partial disclosure of stored computer data including the need for a national legal context for these activities to take place. There are still significant debates on several issues which were addressed in the convention with special interest in the practical implementation—particularly in the area of search and seizure of stored computer data and interception of content data. Section 32b continues to incur significant debate and disagreement relating to direct access by third countries' law enforcement authorities to data stored in other jurisdiction.²⁸ The Article 29 working Group²⁹ identifies the need to obtain the "lawful and voluntary consent of the person who has the lawful authority to disclose the data".

²⁸http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf (last accessed 10 Jan 2015).

²⁹Article 29 Directive 95/46/EC 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 (OJ L 281, 23.11.1995, p. 31) sets up a Working Party on the Protection of Individuals with regard to the Processing of Personal Data. The "Article 29 Working Party" has advisory status and acts independently.

2.3 Conclusion

Self-regulation and co-regulation are powerful strategies in combining the strengths and expertise of multiple stakeholders against a common concern such as child abuse and xenophobia in a new complex medium such as the Internet or the mobile space. However, it can be dangerous if we do not understand the motivations of the various stakeholders involved in the activity, and it is important to balance the needs of appropriate levels of criminal investigations and crime prevention with human rights, family life and freedom of speech as defined in the Universal Declaration of Human Rights³⁰ and the European Convention on Human Rights.³¹ It is important that these competing rights are balanced to avoid suspicion of a lack of transparency and accountability. This can be achieved through open processes and procedures and ensuring appropriate, relevant external measurements of success. Recent disclosures by Edward Snowden on the activities of the US National Security Agency in widespread monitoring have increased concerns about human rights and about self-regulation over-reach. However, these disclosures have also confused the mandate and the activities of national security agencies globally with the legally approved and transparent activities supporting criminal compliance and criminal investigations for illegal online activities and content.

Self-regulation and co-regulation started at a time when there were few dedicated law enforcement operated cybercrime units globally. However, in the last two decades, every national security and national law enforcement agency has comprehensive, expertly trained, agencies that handle complex cyber investigations with high levels of international collaboration when appropriate. This means that there are greater levels of cooperation between the Internet industry and law enforcement and this activity is supported by the Council of Europe guidelines³² on this subject. At the European level, the European CyberCrime Centre (EC3) was established in January 2013 and Interpol continues to ramp up its knowledge and expertise in this area.

Chapter 1 notes that cybersecurity is rather a concept or a process than a result, and trust in relationship between government and private sectors is an intangible issue that cannot be simply enforced or imposed by simply implementing mandatory obligations for sharing information about threats.³³ Chapter 1 describes the evolution of self-regulation and co-regulation after 2005 and the increased attempts at direct regulation.

³⁰<http://www.un.org/en/documents/udhr/>.

³¹http://www.echr.coe.int/Documents/Convention_ENG.pdf.

³²http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/LEA_ISP/default_en.asp (last accessed 4 Jan 2015).

³³Chapter 1, Sect. 1.5.3.

It is reasonable for everyone to debate the nature and style of self-regulation and co-regulation into the future, transparency and accountability requirements and the appropriate balance of cooperation with the role of skilled law enforcement investigations. Otherwise, we will not maintain the trust and support of the Internet users.

Annex—Technology Options: Internet Monitoring and Blocking

Technical solutions for monitoring and blocking have evolved significantly since the beginning of the Internet. There are two main areas of interest including the technical methods of monitoring and blocking and how to specify which content/user is to be monitored/identified.

A comprehensive approach to monitoring requires both the technology itself (hardware, software and interconnections) and ways to specify/identify the specific content to be blocked or monitored. The nature of the content—image, text, video, voice, etc.—first needs to be determined, and it must be decided whether it is required to log records of traffic data (identities of communicating parties) or record copies of communications (message content) or disrupt the communications flow by either preventing the successful completion of the selected communications or by changing the nature of the communications exchange.

Whereas there are complex methods of protecting traffic from eavesdropping or interception using modern tools for encryption, until recently as a result of the alleged widespread monitoring of Internet traffic directly from the fibre-optic cables and major Internet hubs, few Internet companies have adopted encryption for traffic exchange. It is rare that email is encrypted in transit or that data are stored in encrypted format with no access by the hosting provider. In any case, if content encryption is implemented, then because of the design of the Internet, it is difficult to obfuscate Internet traffic records with the intention to bypass blocking or monitoring except with the use of TOR networking (The Onion Router). TOR creates complex Internet traffic paths which then obfuscate the unique patterns of any single traffic pattern which are of interest. Unfettered access to primary international communication cables can support the possibility of decoding such obfuscated patterns.

Child Abuse Material

Let us review the challenges of detecting child abuse material with specific focus on images rather than text, voice or video. Such material must first be created, then distributed on the Internet, downloaded by interested parties and then stored and

viewed. Each of these steps creates both online and offline digital fingerprints and records.

The camera, which records an illegal image, also records additional meta-data about the image which describes the technical photographic context when the image was recorded (light levels, indoor/outdoor, lens aperture and duration of exposure), and modern cameras can record GPS, camera model, camera serial number or camera configuration at the time the image was taken. Recent advances in camera sensors (which offer very high resolutions) permit the identification of a specific camera by calculating the almost unique “dna” of each camera where minor differences and variations on image processing capabilities can permit the identification of a camera by analysing publicly displayed photographs with non-public illegal images. The image of a modern digital camera is stored in a memory storage device which can also be forensically analysed for digital fingerprints. The image storage structure is different for different brands of cameras, and direct access to the storage media can yield many useful clues for a criminal investigation.

Once the image is created, the image will be distributed on the Internet. It might be first edited, changed or obfuscated using software or hardware to destroy, corrupt or delete digital fingerprints and, in extreme cases, this can be successful. However, even in these difficult cases, the computer where this work was conducted will contain forensic records of activities—software installed and used, image files accessed, files edited, use of Internet programmes and often detailed timeline of activities which occurred on the computer. Forensic analysis can detect image edits and updates (morphed images). The records of Internet access to upload the content onto the Internet creates a complex web of digital artefacts on the device used to upload the data from and also creates a complex range of log records on the local and intermediate Internet service providers.

The image can be accessed, viewed and downloaded from persons located across the world. There will be digital records and fingerprints on the intermediary service providers and the end-user Internet service provider and on the local network and the local device used to initiate the Internet activity.

The image can be stored in many different formats supplemented by compression, encryption or hiding techniques. It can be stored in many different types of media and with direct, indirect or no network access. It can be stored in cameras, tv recorders, game players, children’s toys, health monitoring devices, etc. in addition to a wide variety of computing and mobile devices. Stored data do not have to be static and can be transferred across international and jurisdictional boundaries on random or regulated schedules or can be divided across many different international storage locations.

Of course, if it is possible to access computing devices remotely or if it is possible to have unrestricted access to network cables at a national and international level, then there are serious concerns about the level of trust which can be placed on digital evidence since with enough knowledge of computing systems and application structures available to digital forensic scientists, it would be possible to surreptitiously place believable difficult-to-refute evidence on any system and ensure the supporting traffic logs are recorded on intermediary systems.

If we study the actual images that are considered the image of a crime scene where the abuse of a child takes place, we need to work to determine several critical pieces of information from the image analysis. We need to identify the location where the image was taken. We need to identify the victim or victims in the photograph so that the victim can be rescued from a damaging situation and provided with treatment and support. We need to identify the perpetrators who committed the crime and the identity of the photographer if different. The image can be analysed to identify any known product brands in the image which can identify the continent, country and region or even shop where the product was sold and bought. For example, there was one image where the boxes of computers previously purchased were recorded in the image which almost offered a detailed view of a barcode of the purchaser account details. Another image when abuse occurred in a child's playground was identifiable from the type, range, colour and layout of the playground equipment. The image can contain artefacts of telephones, power sockets, newspapers, magazines, etc. which can be used to narrow down the search to a location for more traditional methods of investigation. The clothes worn by the victims and the shadows of the perpetrator can offer clues to the investigation.

These techniques described in the previous paragraphs apply to static text images, but there are evolving techniques that offer similar levels of forensic analysis for other types of content such as video, voice or text material.

Specifying Content

To specify which content is illegal or not illegal, there should be a trained and skilled expert making the evaluation of the alleged illegal content against a specific legislative provision. In the area of child pornography (the usual legal term for child abuse material), the major primary definitions are in the Council of Europe Conventions on Cybercrime and Protection of Children against Sexual Exploitation and Sexual Abuse and the European Commission Directive on Certain legal aspects of information society services, in particular electronic commerce and Directive 2011/93/EU of the European Parliament and of the Council on combating sexual abuse and sexual exploitation of children and child pornography. These documents are then supported by national law which defines the exact nature of child pornography and child abuse. Images, text, videos, voice and illegal activities are clearly defined, and any content on the Internet which is suspected of being child abuse material needs to be evaluated according to these standards. In an ideal world, content would be evaluated in a clearly specified judicial process, but due to the speed of movement on the Internet, such procedures, although still used for the prosecution of individuals, were found to be inadequate for content on the Internet. Often the material is initially assessed by the Internet hotlines created across the world which pass suspect material to law enforcement who make the determination whether material is likely to be illegal.

Today Interpol³⁴ and US NCMEC³⁵ (National Centre for Missing and Exploited Children) host a list of the worst images of child abuse which have been discovered and share this list of images with law enforcement agencies across the world. The national law enforcement agencies then share this list with trusted Internet service providers to enable them to detect the upload or download of such images from their networks.

When material is deemed to be illegal, attempts have been made to ensure that this material is not further re-distributed on the Internet using blocking technologies. The list of known illegal images is also used to make legal search and seizure and forensic analysis of computer networks, hosts and storage media faster by using the list to compare against currently hosted and stored files to determine if any known illegal images are among the seized or monitored material.

The creation of the list is an important role that requires oversight and accountability since it would be possible to include any type of material on the list and there have been accusations in the past that list maintained have included material on the list which is not illegal but might be considered to be inappropriate by conservatively minded individuals.

The list itself is a special technical challenge. In fact, there are several lists that exist for different Internet services.

There is a list of known keywords used by paedophiles to search for child abuse material on search engines. This list is distributed to search engine providers to prevent users from using their services to access illegal content.

There is a list of known websites which have regularly hosted illegal material. This list can be used both by search engine providers and by hosting providers and blacklisting inappropriate sites that are blocked by host-based anti-malware software. This list can include a list of IP addresses or domain names.

The third list is a list of known illegal images that have been detected during investigations by law enforcement across the world. It would not be legal or indeed morally appropriate to distribute the exact images of child abuse. Instead, alternative methods of specifying content are required. Such methods need to be precise and accurate so that they uniquely specify an image of known child abuse and cannot accidentally refer to other legal content. The method is known as digital image fingerprinting. A fingerprint is a computer algorithm which calculates a one-way numerical code which uniquely identifies each specific image. The fingerprint unique code is compared against the calculated code for a suspect image. If the generated code matches one that is on the list of illegal content, then we can be sure that the images are identical.

One problem with the approach of seeking identical matches between images is that minor changes in the suspect image (cropping, resizing, re-colouring, etc.) means that the image fingerprints will be different from the ones on the list of

³⁴<http://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children> (last accessed 4 Jan 2015).

³⁵<http://www.missingkids.com/Exploitation/Industry> (last accessed 4 Jan 2015).

known illegal content. New approaches have been adopted to deal with such situations. One such technique is called PhotoDNA³⁶ developed by Microsoft Research in collaboration with Dartmouth College. According to Microsoft³⁷ *“PhotoDNA enables analysts to calculate the unique digital signature of an image and then match that signature against those of other photos. The PhotoDNA ‘robust hashing’ technique differs from other common hashing technologies because it does not require the image’s characteristics to be completely identical to reliably find matches, thereby enabling matches to be identified even when photos are resized or similarly altered”*. Of course, when images are not directly matched using specific matching, any matches suggested by PhotoDNA software need to be verified by human eye for further criminal investigation.

Microsoft, Facebook and other international service providers now use PhotoDNA with lists provided by Interpol or NCMEC to compare all images uploaded to their services against the known list of illegal content. Any content that matches is forwarded to law enforcement for investigation.

As regards video content, there are separate techniques developed by Videntifier from Iceland³⁸ in collaboration with Interpol and others to create methods of uniquely identifying videos.

The major limitation of all these approaches is that they can only report on known content. They cannot easily detect new material that has not been seen before or investigated by law enforcement. However, there are initiatives to detect content which has not been seen before through complex image analysis with attempts to detect images based on skin tone, title and sharp analysis. Further details are available in the FIVES: Forensic Image and Video Examination Support³⁹ project description and iCop: Identifying and Catching Originators in P2P Networks.⁴⁰

Whereas all these examples have used the area of child abuse as an example, many states are concerned about a diverse range of online content and activity. Many states are also concerned about extreme adult content, many are concerned about online incitement to terrorism, and many are concerned about illegal online drugs or gambling.

There are concerns that service providers are being drawn into areas of behaviour which are not sufficiently transparent or accountable and have a direct impact on human rights and rights to family life and rights to freedom of expression. In some countries, criticising the state is a criminal offence. The EDRI document

³⁶http://www.microsoft.com/global/en-us/news/publishingimages/ImageGallery/Images/Infographics/PhotoDNA/flowchart_photodna_Web.jpg (last accessed 4 Jan 2015).

³⁷<http://www.microsoft.com/en-us/news/presskits/photodna/docs/PhotoDNAFS.doc> (last accessed 4 Jan 2015).

³⁸<http://www.videntifier.com/news/article/advanced-video-and-image-analysis-in-interpol-child-abuse-database> (last accessed 4 Jan 2015).

³⁹http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SIP-2008-TP-131801 (last accessed 4 Jan 2015).

⁴⁰<http://scc-sentinel.lancs.ac.uk/icop/> (last accessed 4 Jan 2015).

human rights and privatised law enforcement “looks at the extent to which ‘voluntary’ law enforcement measures by online companies are serving to undermine long-established fundamental rights principles and much of the democratic value of the Internet”.⁴¹

Different Services

Not all Internet services are the same. It has been outlined earlier the complex range of services. Each service has different capabilities for oversight, monitoring and detecting criminal activity. Email is different from peer-to-peer, and social network websites are very different from search engine providers. Whereas many of these services play a role in combating illegal online activity and content, there are also many methods to evade detection and circumvent blocking initiatives.

Appendix I

List of Newsgroups from Metropolitan Police 26 August 1996 requested to be blocked.

```
alt.binaries.pictures.boys
alt.binaries.pictures.childerotica.female
alt.binaries.pictures.childerotica.male
alt.binaries.pictures.children
alt.binaries.pictures.erotic.children
alt.binaries.pictures erotica child
alt.binaries.pictures erotica child.female
alt.binaries.pictures erotica child.male
alt.binaries.pictures erotica children
alt.binaries.pictures erotica.lolita
alt.binaries.pictures erotica.pre-teen
alt.binaries.pictures erotica.teen.fuck
alt.binaries.pictures erotica.young
alt.binaries.pictures.lolita.fucking
alt.binaries.pictures.lolita.misc
alt.sex.boys
alt.sex.children
alt.sex.fetish.tinygirls
alt.sex.girls
alt.sex.incest
```

⁴¹<https://edri.org/human-rights-and-privatised-law-enforcement/> (last accessed 4 Jan 2015).

alt.sex.intergen
alt.sex.pedophile.mike-labbe
alt.sex.pedophilia.
alt.sex.pedophilia.boys
alt.sex.pedophilia.girls
alt.sex.pedophilia.swaps
alt.sex.pedophilia.pictures
alt.sex.pre-teens
alt.sex.teens
alt.sex.weight-gain
alt.fan.cock-sucking
alt.binaries.pictures.voyeurism
alt.binaries.pictures.lolita.fucking
alt.binaries.pictures.erotica.voyeurism
alt.binaries.pictures.erotica.young
alt.binaries.pictures.erotica.uniform
alt.binaries.pictures.erotica.urine
alt.binaries.pictures.erotica.teen.fuck
alt.binaries.pictures.erotica.uncut
alt.binaries.pictures.erotica.spanking
alt.binaries.pictures.erotica.teen.female.
masturbation
alt.binaries.pictures.erotica.pornstars
alt.binaries.pictures.erotica.pre-teen
alt.binaries.pictures.erotica.oral
alt.binaries.fetish.scat
alt.binaries.pictures.erotic.anime
alt.binaries.pictures.erotic.centerfolds
alt.binaries.pictures.erotic.senior-citizens
alt.binaries.pictures.erotica.animals
alt.binaries.pictures.erotica.art.pin-up
alt.binaries.pictures.erotica.breasts.small
alt.binaries.pictures.erotica.butts
alt.binaries.pictures.erotica.cheerleaders
alt.binaries.pictures.erotica.disney
alt.binaries.pictures.erotica.fetish.feet
alt.binaries.pictures.erotica.fetish.hair
alt.binaries.pictures.erotic.senior-citizens
alt.binaries.pictures.erotica.teen
alt.binaries.pictures.erotica.male.anal
alt.sex.pedophile.mike-labbe
alt.sex.masturbation
alt.sex.fetish.tickling
alt.sex.fetish.waifs
alt.sex.fetish.watersports

alt.sex.fetish.wrestling
alt.sex.first-time
alt.sex.fetish.girl.watchers
alt.sex.homosexual
alt.sex.incest
alt.sex.intergen
alt.sex.jp
alt.sex.magazines
alt.sex.masturbation
alt.sex.movies
alt.sex.necrophilia
alt.sex.pedophilia
alt.sex.pictures
alt.sex.pictures.female
alt.sex.pictures.male
alt.sex.services
alt.sex.spam
alt.sex.spanking
alt.sex.stories
alt.sex.strip-clubs
alt.magazines.pornographic
alt.magick.sex
alt.personals.spanking.punishment
alt.sex.
alt.sex.anal
alt.sex.bestiality
alt.sex.bondage
alt.sex.breast
alt.sex.enemas
alt.sex.exhibitionism
alt.sex.fat
alt.sex.fetish.diapers
alt.sex.fetish.fa
alt.sex.fetish.feet
alt.sex.fetish.hair
alt.sex.fetish.orientals
alt.binaries.multimediaerotica
alt.binaries.pictures.boys
alt.binaries.pictures.children
alt.binaries.pictureserotica
alt.binaries.pictureserotica.amateur.d
alt.binaries.pictures.amateur.female
alt.binaries.pictures.amateur.male
alt.binaries.pictureserotica.anime
alt.binaries.pictureserotica.bestiality

alt.binaries.pictureserotica.blondes
alt.binaries.pictureserotica.bondage
alt.binaries.pictureserotica.cartoons
alt.binaries.pictureserotica.female
alt.binaries.pictureserotica.furry
alt.binaries.pictureserotica.gaymen
alt.binaries.pictureserotica.male
alt.binaries.pictureserotica.orientals
alt.binaries.pictureserotica.pregnant
alt.binaries.pictureserotica.teen
alt.binaries.pictureserotica.teen.d
alt.binaries.pictures.girlfriend
alt.binaries.pictures.girlfriends
alt.binaries.pictures.girl
alt.binaries.pictures.horny.nurses
alt.binaries.pictures.pictures.nudism
alt.binaries.pictures.tasteless
alt.homosexual
alt.sex.swingers
alt.sex.telephone
alt.sex.trans
alt.sex.wanted
alt.sex.watersports
alt.sex.bestiality.pictures
alt.sex.children
alt.sex.cu-seeme
alt.sex.fetish.scat
alt.sex.fetish.tinygirls
alt.sex.fetish.wet-and-messy
alt.sex.oral
alt.sex.orgy
alt.sex.pedophilia.girls
alt.sex.pedophilia.pictures
alt.sex.pictures.d
alt.sex.stories.gay
alt.sex.stories.tg
alt.sex.super-size
alt.sex.tasteless
alt.sex.teens
alt.sex.video-swap
alt.binaries.pictureserotica.black.male
alt.binaries.pictureserotica.children
alt.sex.sm.fig

References

1. Akdeniz Y (1997) Governance of pornography and child pornography on the global internet: a multi-layered approach. In: Edwards L, Waelde C (eds) *Law and the internet: regulating cyberspace*. Hart Publishing, Oxford, pp 223–241
2. European Commission (1996) *Illegal and harmful content on the internet*. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions. COM (96) 487 final, 16 October 1996
3. Akdeniz Y (1997) ‘Policing the Internet’, Conference Report, 1997 (1) *The Journal of Information, Law and Technology (JILT)*. http://elj.warwick.ac.uk/jilt/bookrev/97_1/pol/. New citation as at 1/1/04: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1997_1/akdeniz2/
4. Council of the European Union (1997) Resolution of the Council and of the Representatives of the Governments of the Member States, meeting within the Council of 17 February 1997 on illegal and harmful content on the Internet Official Journal C 070, 06/03/1997 P. 0001–0002
5. Clinton WJ, Gore Jr, A (1997) *The global information infrastructure (GII)—The Framework*. <http://clinton4.nara.gov/WH/New/Commerce/read.html>. Last accessed 8 Dec 2014
6. European Union Ministers (1997) European Ministerial Conference entitled “Global Information Networks: Realising the Potential”, held in Bonn from 6–8 July 1997. Declaration available on http://web.mclink.it/MC8216/netmark/attach/bonn_en.htm#Heading01. Last accessed 7 Dec 2014
7. Department of Justice, Equality and Law Reform, Ireland (1998) Working Group on Illegal and Harmful Use of the Internet, First Report of the Working Group. http://www.justice.ie/en/JELR/Pages/Illegal_use_of_the_Internet_report. Last accessed Dec 14
8. European Parliament (2013), COM (2013) 48: Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union Available on <http://eur-lex.europa.eu/procedure/EN/202368>. Last accessed Dec 14
9. UNESCO (1999) Experts Meeting on Sexual Abuse of Children, Child Pornography and Paedophilia non the Internet : an international challenge UNESCO, Paris Room II, Background Document. (CII-98/CONF. 6051 (E) <http://unesdoc.unesco.org/images/0011/001147/114751Eo.pdf>. Last accessed 9 Dec 2014
10. European Parliament (1999) Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999D0276&from=EN>. Last accessed 8 Dec 2014
11. European Parliament (2003) DECISION No 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 amending Decision No 276/1999/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003D1151&from=EN>. Last accessed 8 Dec 2014
12. European Commission (2003) Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions concerning the evaluation of the Multiannual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors 03.11.2003 COM(2003) 653 final. Available on <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52003DC0653&from=EN>. Last accessed 8 Dec 2014
13. European Parliament (2005) DECISION No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005D0854&from=EN>. Last accessed 8 Dec 2014

14. European Commission (2007) Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions COM/2007/0496 final—Available on <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52007DC0496>. Last accessed 14 Dec 2014
15. European Parliament (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce. Official Journal L 178, 17/07/2000 P. 0001–0016. Available on <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML>. Last accessed 14 Dec 2014
16. Council of Europe (2001) Convention on Cybercrime signed in Budapest on 23.XI.2001 (ETS No. 185) Available at <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>. Last accessed 14 Dec 2014
17. Bertelsmann Foundation (1999) Self-regulation of Internet Content by Dr, Marcel Machill and Jens Waltermann

Self- and Co-regulation in Cybercrime, Cybersecurity
and National Security

Tropina, T.; Callanan, C.

2015, IX, 100 p. 1 illus., Softcover

ISBN: 978-3-319-16446-5