THIRD PARTY RESPONSIBILISATION FOR CRIME CONTROL -TELECOMS AND FINANCIAL POLICING

*Keiji Uchimura**

I. ABSTRACT

Technological developments, globalisation and diversification of industrial services have weakened the technical and social control of crime and indirectly facilitated more serious crime, endangering the law enforcement mission. To meet these challenges, law enforcement authorities have developed a relationship with industries. For example, the telecommunication industry is obliged to provide interception capabilities. In the same way, financial institutions are required to lodge Suspicious Transaction Reports. These are types of 'responsibilisation' of the industries, as David Garland termed such political strategies of the state. The aim of this paper is to shed light on the actual conditions of the relationship and to find out keys to improve the relationship. Based a review of the literature and the recognition of limits of such open sources of telecoms and financial policing, interviews were conducted in Belgium, Hong Kong, Ireland, Singapore and the UK. It was concluded that the keys to crime control and socially sound development of industry are mutual understanding and collaboration between law enforcement and industry rather than controlling the industries unilaterally. In particular, it became clear that a good relationship with financial institutions is achieved through the upstream flow of information on the progress of criminal investigation. On the other hand, finding a successful model in telecoms policing is still a difficult problem for the time being. The root of trouble with the relationship is the difficulty in determining who should pay the cost of telecoms policing. In order to ameliorate the circumstances, the author proposes applying technical standardisation schemes.

Concerns about privacy and the resolution of costs might arise through such standardisation processes by collaboration of all parties in question.

II. INTRODUCTION

Cyberspace is not only the scene of cybercrime but is also tainted with 'traditional' crime.[1] The capabilities of telecoms policing typified by interception and data seizure have increasingly become vulnerable with the advance of technology and the expansion of services. Thus, the public police cannot appropriately cope with policing needs in cyberspace by themselves. Instead, having a universal relationship to crime facilitation and inhibition, the private telecommunications (telecoms) industry has been persuaded and compelled to assist in measures that are not automatically in its own short-term economic interests. Interestingly, almost the same pattern is recognised in the relations between financial policing and the financial industry.

Focusing on telecoms and financial policing, this paper will shed light on the actual conditions of the relationship and find keys to improve the relationship. Throughout this paper, the term 'telecoms policing' stands for any policing activities conducted (not necessarily by the public police) in cyberspace for preventing, detecting, investigating and remedying (not necessarily cyber-) crime.

To begin with, various aspects of the relationship between policing authorities and the telecoms industry are reviewed in the next chapter. Chapter IV deals with issues of financial policing and then these are compared with telecoms policing matters. Proposals are made based on theoretical discussions in the concluding chapter in weaving the findings of the author's interviews with foreign law enforcement officials.

III. RESPONSIBILISING TELECOMS POLICING

A. The Interception Law in Japan

The 'Telecommunication Interception for Criminal Investigation Law' (Interception Law)[2] was enacted in

* Professor of Applied Technology, Police Info-Communications Academy, National Police Agency, Japan.

1 See Council of Europe (2001: para. 5).

2 The author concerned himself with the law by liaising with the telecoms industry and by settling on the procedural details of the due process of the Law.

2000 in Japan. The aim of the law is to tackle organised crime by authorising law enforcement agencies to intercept telecommunications related to organised crime. The history of such investigative method in Japan is shorter than the legislative traditions in Western countries.[3]

1. Precedents: Substituting *'Inspection' for 'Interception'*

There were five precedential and quite exceptional cases before the legislation (Homusho 1998: 29-34). The courts diverted the 'inspection'[4] procedure issuing warrants that permitted the police to 'inspect' the telecommunications contents. These cases were characterised by the system called Tachiainin (Presence of the Responsible). The purpose of the system is to guarantee procedural appropriateness (Inoue 1997: 77). The court applied the principle that police should ensure the presence at the site of personnel of the telephone company concerned (or, failing that, local government personnel).[5] However, the telephone company staff refused, in all five cases, to become tachiainin arguing that such co-operation contradicts the industry's legal responsibility on confidentiality of communications.[6] Consequently, the police had to depend on local government officials instead of telecommunication experts.

2. A Challenging Situation: Inheritance of the Tachiainin system

The tachiainin system was handed over and developed as a new distinctive due process for interception. The law concerning the tachiainin system stipulates that-[7]

> in case interception is to be executed, a person who is responsible for the part of the telecommunication means or any suitable substitute shall be present on the spot. If such persons are not available, a local government official shall be present.

Thus, the primarily eligible persons to be tachiainin are the staff of the telecoms service provider involved. The presence of tachiainin at all times is the most important part of the procedure. The Criminal Procedure Code allowed the non-attendance of tachiainin for exceptional circumstances of non-availability.[8] However, such an exceptional clause was removed from the Bill to place a responsibility on tachiainin to carefully watch the process of interception.[9] Unlike the precedents, they are prohibited from monitoring the communication contents and neither the right nor the responsibility of stopping interception is placed on them. In this sense, the new system sets a lighter responsibility for tachiainin than that of the inspection-interception scheme.

According to the testimony of a government delegate of the Yuseisho (Ministry of Posts and Telecommunications, MPT),[10] tachiainin have two important roles. The first function is to be present during the entire process at the scene in light of the need for the telecoms carrier to maintain their entire service without any adverse effect. Secondly, being tachiainin is an obligation for telecoms service providers, forming a part of the due process of the law. The delegate further set forth that telecoms service providers are fundamentally responsible to carry out duties of tachiainin in order to keep the integrity of their own telecommunication business.

Notwithstanding, the telecoms industry has speculated that the burden[11] of constantly seconding

---

3 For example the Interception of Communication Act *1985* in the UK and Title III of the Omnibus Crime Control and Safe Streets Act of *1968* in the US.

4 Article 218 of the Criminal Procedure Code.

5 Tachiainin were permitted to monitor the telephone conversation in common with investigators. In addition, they were then requested to disconnect temporarily the branched line to disable it from monitoring and recording if the call contents were not related to the crime (Homusho 1998: 29-34).

6 "Soshiki Hanzai Hoan no Yukue" (Organised Crime Bill's Whereabouts). The evening issue of Mainichi Shinbun, 21st May 1999. http://www.mainichi.co.jp/eye/feature/article/digital/55/55_4.html.

7 Article 12, para. 1 of the Interception Law.

8 Article 114, para. 2 of the Criminal Procedure Code.

9 Statement of Sasagawa Takashi, a member of the House of Representatives, before the Legal Committee, House of Councillors, 29th June 1999.

10 Testimony before the Legal Committee, House of Representatives, 19th May 1998.

11 "Tachiainin Keihi mo'Jigyosha de'"('Operators' are compelled to pay tachiainin costs). The morning issue of Asahi Shinbun, 13th August 2000, http://www.asahi.com/tech/jiken/20000813b.html. However, the validity of the media's articles about the Interception Bill of the media was questioned. Seko, Hiroshige, a lawmaker who had been employed by the common carrier (NTT), indicated (before the Legal Committee, House of Councillors, 13th July 1999), with evidence, that the article contained false information and was biased.

personnel over a long period might be too heavy to bear. A newspaper article appeared just two days before the Law came into force criticising the heaviness of the burden . It quoted the view of the compliance officer of a fixed-line telephone company that it would be difficult to station tachiainin if interception is enforced one after another. The article also included the comment of a mobile phone operator expressing the view that they couldn't refuse their tachiainin duties because the company had a social responsibility to do so. At least in the short period immediately after the law became effective and when the author liaised with them for preparation, they repeatedly requested the police to release them from their duties of tachiainin because they thought it would interfere with their business.

3. Interception Capabilities

Another concern about interception investigation was the costs of development to facilitate telecoms interception. Hitherto, Japanese legislation provided neither a legal obligation for service providers to install interception capabilities nor a legal claim for the costs of doing so.[12] Lawmakers permitted the police to make requests to the industry provided they were non compulsory and not excessive. Since the legal and political circumstances in Japan are quite different from other countries,[13] it is inevitable that the technical implementation for interception in Japan is limited in extent. Although, the cause and effect cannot be fully discussed, it can be recapitulated that the technical difficulties combined with operational barriers resulted in the limited applicability of the law.[14] Nevertheless, the imbalance between telecoms policing needs and capabilities is a globally common issue.

B. Global Difficulties and Responses to Telecoms Policing

1. The Era of Analogue Technology and the Monopolised Supplier

Traditionally, the technical methods of telecoms policing were relatively simple. As for telephone interception, call content was available by the following means (see Grabosky and Smith 1998: 21-22). First, a pair of copper cables were branched off near the local switch. Then the branch was extended to the interception site. Traffic data, e.g. call length and dialled numbers, were logged in correlation with subscriber data for billing purposes (Lloyd 2000: 179-180). Dialled numbers were also obtainable, without assistance of telephone service providers, by attaching a device called the 'pen-register' to the branch (Diffie and Landau 1999: 117).

Unlike the Internet or mobile phone services, subscribers' static data of fixed line services were easily accessed by lawful powers because the customers are literally connected. Another facilitating factor was the monopolisation of services. As Grabosky and Smith (1998: 206) pointed out, '[e]nlisting the co-operation of a single, large organisation was a relatively routine matter.' Thus, it can be summarised that the telecoms policing of early days was easy.

2. Technical Developments and Increasing Anonimity

Because of advances in the technology and popularity of services, the importance of data handled by the industry has grown. Additionally, technologies needed for telecoms policing of modern systems have become far more difficult (see Diffie and Landau 1999: 97-99). Furthermore, the global popularity of mobile phones and the Internet has brought about challenging situations. It is almost impossible, and arguably inappropriate, for public police to install functions by themselves within the huge networks, whether confidentially or not. There seems to be no other solution than pre-installing capabilities friendly for policing (Diffie and Landau 1999: 116).

To make matters worse, digital technology is applied in almost all telecoms systems removing biological features of users (Council of Europe 2001: para. 62). Diversified services have also deteriorated. The traffic

---

12 Testimony of Matsuo, Kunihiro, before the Legal Committee, House of Councillors, 29th July 1999.

13 For example, the Communication Assistance for Law Enforcement Act of 1994 (CALEA) of the US places telecommunication providers under an obligation to be equipped with interception capabilities. Similarly in the UK, the Regulation of Investigatory Powers Act 2000 stipulates in article 12 that persons providing public telecommunications services are liable to assist by interception capabilities.

14 After two Annual Interception Reports reported that there were no cases, the first productive report was submitted to the Diet in February 2003. It disclosed that four interception warrants for mobile phones were enforced for drug dealing cases in the previous year. See http://www.npa.go.jp/keiji/boujyuhouoku.htm.

data of the modern systems are not usually recorded if the services are flat-rated or free of charge because they are not needed for billing purposes (APIG 2003: para. 128). Similarly, the allocation data of IP addresses (subscriber data) and the history of IP addresses of destination (traffic data) were also immediately deleted by Internet Service Providers (ISPs) because they are regarded as valueless (Council of Europe 2001: para. 29). In addition, many free email services are accessible to anybody. Such services are not only free of charge but also require little proof of identity. The most problematic services are 'anonymous remailers' (Mostyn 2000: 81-82). The problem of anonymity is also found in pre-paid mobile systems (Denning and Baugh 1997: 128).

3. International Responses - The Requirements

In parallel with domestic struggles, already discussed, remarkable international efforts have been made since the mid 1990s mainly in order to regain interception capabilities. The first initiative was started under the EU and bore fruit as the Council Resolution in 1995. A set of 'requirements' of law enforcement agencies for telecoms policing, often referred to as the 'International User Requirements (IUR)', is acknowledged in the first half of the resolution. Then in the latter half, member states are required to implement the requirements (The Council of the European Union 1996). This resolution would be epoch-making for it pioneered an international concern about capabilities of telecoms policing.

4. International Responses - Standardisation

An international effort was also made by the ITU (International Telecommunication Union) adopting Resolution 1115, 'International Harmonization of Technical Requirements for Legal Interception of Telecommunications'. The motivation for the resolution was 'that the costs of legal interception capability and associated disruptions can be lessened by providing for the capability at the design stage'.[15] Although the ITU has made no progress since 1997, the regional standardisation has been active in Europe. The ETSI (European Telecommunications Standards Institute) has established standards relating to lawful interception.[16] The reason for the difference in productivity between the two projects is that, whereas the ITU could not co-ordinate the diverse political and economic conditions of members, the law enforcement needs and industrial efforts to respond to them have been matched among European countries (Tsuchiya 2001: 16). Standardisation in the ETSI has produced satisfactory results not only in the economies of scale but also in removing trans-border barriers among jurisdictions and markets with different legal requirements (p. 16).

5. International Responses - Countermeasure against Cyber-crime

Members of the Council of Europe and some extra regional countries signed the *'Convention on Cybercrime'*. The significance of the treaty for telecoms policing is that it requires states to establish new powers to enable 'the expeditious preservation of' existing computer data, including traffic data.[17] Backed by the provision, the Japanese government is preparing domestic legislation to create new investigative powers to request telecom service providers to retain traffic data up to ninety days.[18]

However, the industry has opposed the data retention policy because it costs a great deal of money. As the WITSA (World Information Technology and Services Alliance) (2000) appealed 'as the global voice of the IT industry' to governments in the statement for the Draft Convention -

> to avoid imposing new requirements [for data preservation] on ISPs that result in significant financial burdens on their operations. Such added costs will ultimately affect the access costs of end users, and may negatively affect the growth of Internet usage.

C. Case Studies of Telecoms Policing

1. Legal Solution: Internet Auction Providers' New Responsibility

The first case study deals with the world's first legal regulation for on-line auction providers. The

15 See http://www.itu.int/council/index97/1997/135/135.html.
16 See http://www.etsi.org/.
17 Article 16 of the Convention on Cybercrime: Explanatory Report.
http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.
18 See http://www.moj.go.jp/SHINGI/030324-2.html.

Amendment of the Second-hand Dealing Law went into effect in April 2003 in Japan.[19] The amendment requires any online auction provider (1) to notify police as a 'service provider of second-hand articles auction mediation' (an Auction Mediator), (2) to report to the police if any article on the auction block is suspected of being a stolen item, and (3) to take the appropriate action to halt the auction if the article is obviously recognised as a stolen item.

The amending process was tangled. The industry opposed the bill partly because the burden of inspecting the suspiciousness of articles is too heavy.[20] Moreover, lawmaker Yoko Tajima's criticism of the bill was as follows.[21]

> Police must be admitting the ineffectiveness of their cyber-patrol to lobby this bill. [. . .] Presumably, the real intention of the crafty bill might be to divert the responsibility of impotent police onto the industry's shoulder.

2. Telecoms Policing in the UK

Secondly, the measures for telecoms policing in the UK are examined. The *Regulation of Investigatory Powers Act 2000* (RIPA) established the powerful and expanded legal framework of telecommunication interception. In addition, unlike Japanese legislation RIPA provides that the operational costs for the implementation of individual interception warrants are paid in full by the government. Presently discussions are going on between the industry and the Home Office on fair compensation from the government for installing interception capabilities in compliance with section 13 of RIPA. Sutter (2001) argues that due to the compliance burden, British ISPs are at risk in the domestic market because of the challenge by competitors based outside the jurisdiction who might provide cheaper services.

The *'Anti-Terrorism, Crime and Security Act 2001'* (ATCS) legalising communications service providers (CSPs) to retain any sort of communications data on a voluntary basis to enable anti-terrorism measures.[22] ATCS has been criticised because the government disregarded groundwork with the industry (Thomas 2002). Further, a Parliamentary group pointed out how the system is economically not feasible. Rather than voluntarism, they made the counterproposal of a reasonable 'Data Preservation' system- to comply with a request to preserve certain communications data (APIG 2003: para. 179).

3. *Paralegal* Solution (1): 'Know Your Customer' for Prepaid Phones

The next case study is about the crime investigation and prevention measure taken by the Japanese industry. This case was characterised as being of a *paralegal* nature, achieved through administrative guidance.

When a pre-paid mobile phone was used in a kidnapping for ransom case in 1999, the police had difficulty in investigating the case because of the anonymity of the user. In response, the *Keisatsucho* requested mobile operators to collect user identification for crime prevention and the maintenance of investigative capabilities.[23]

The industry held a wait-and-see policy as the first response with informal and theoretical support from the Yuseisho, the regulating authority. According to their argument, the customers' identity information for *pre*-paid services is not needed for billing purposes by definition. Thus, it was considered that the collection of such *unnecessary* information was prohibited by the Privacy Guideline for Telecommunications Business. In addition, the industry contended that collecting such data would be fatal to the service since the convenience of the service is its raison d'etre.

---

19 See http://www.npa.go.jp/safetylife/seiankis9/kobutu.htm.
20 See http://www.watch.impress.co.jp/internet/www/article/2002/0315/npa.htm.
21 Testimony of Tajima, Yoko, a member of the House of Councillors, before the Cabinet Committee, House of Councillors, 19th November 2003.
22 Anti-Terrorism, Crime & Security Act 2001: Summary.
http://www.homeoffice.gov.uk/oicd/antiterrorism/atcsa.htm.
23 "Keitai Denwa: Tokumei no Kyoki" (Mobile phone: an anonymous weapon). Morning issue of Asahi Shinbun, 26th April 2000. http://www.asahi.com/tech/jiken/20000426a.html.

An imitative kidnap case, using a more sophisticated technique, occurred four months later. The *Keisatsucho* made the same request again and wanted the operators to act without delay. The reaction of the Minister of *Yuseisho*, to this was to report, a few hours later, his solution to these kidnap cases as follows.[24]

> Pre-paid mobile phones were abused in the kidnap case committed in December last year and the case in Kanagawa Prefecture this time. I apprehend this situation as a serious social problem. Therefore we have just instructed the industry to devise immediate measures against this matter taking privacy concerns into consideration since the service is a sort of disposable-type. In this context, on the grounds that a serious social evil has arisen from this service through a variety of crimes, not to speak of drug dealing, we would like to discuss immediately the government's countermeasures [. . .].

Under the guidance of the Yuseisho, the industry then began to collect identity data by checking photo identification at shop fronts on the purchase of handsets.[25] According to a Yuseisho official, a modified interpretation of the Guideline made available such a measure. In other words, 'preventing crime' and 'keeping a record to provide against a time of need' were newly authorised to be necessary which allowed the telecoms to avoid potential liability for the infringement of privacy requirements.

4. Paralegal Solution (2): the Anti-mobile Theft Initiative

The last case study is the anti mobile phone theft initiative in the UK. The chronological development of this case is somewhat similar to the above mentioned case; it appears that the escalation of the serious situation brought turning points in both cases.

The Home Office worked on mobile telephone companies to take measures to deny the benefits of mobile phone theft (see Clarke 1997: 23). In January 2001, the government began to request mobile operators to block phone calls from stolen handsets. Whereas three new operators complied with it, two refused. The reasons for the non-compliance were reportedly that the timing of upgrading network systems was approaching and 'customers [were] not demanding it'.[26]

The threat of mobile phone theft and the operators' refusal to comply attracted media concern since the Home Office publicised the results of research into 'mobile phone theft' (Harrington and Mayfew 2001) a year later. A Home Office spokesman revealed that the government has the legislative option of forcing the industry to install technical measures to deter mobile phone theft as a last resort.[27] In addition, they criticised the operators for being unethical:[28]

> [N]etwork operators, as well as criminals, benefit from the problem. They estimate that [they] make tens of millions of pounds each year through calls made via stolen phones. [. . .] [The only party to be hurt is] the customer - and [the mechanism] actually benefits the network because people are still paying for airtime, even if they do so on a stolen handset - they seem to have lost the knack of throwing millions of pounds at the problem.

Just a week after the article appeared, the two mega-carriers simultaneously announced their adoption of the measure to bar calls from stolen handsets and to help to trace them.[29]

IV. THE COUNTERPOINT: FINANCIAL POLICING

A. Overview

This chapter will review financial policing typified by Anti Money laundering (AML) measures as the counterpoint to telecoms policing and examine how these policing schemes resemble each other.

---

24 Testimony of Yashiro, Eita, before the Budget Committee, House of Councillors, 25th April 2000.
25 "Pre-paid Shiki Keitai Denwa ni Kansuru Taiosaku" (Safeguard of Pre-paid Mobile Phone). NTT DoCoMo, 5th May 2000. http://www.nttdocomo.co.jp/new/contents/00/whatnew0512.html.
26 "Phone Firms Defend Security Record", BBC, 8th January 2002.
http://news.bbc.co.uk/1/hi/uk/1749215.stm.
27 Ibid.
28 "The Key to the Mobile Phone Theft Epidemic" Guardian, 2nd February 2002.
http://www.guardian.co.uk/Print/0,3858,4348454,00.html.
29 "Ministerial Statement in Response to Vodafone and mmO2 Announcement on Mobile Phones". Government News Network, 8th February 2002. http://www.nds.coi.gov.uk/coi/coipress.nsf/.

B. Co-operation of the Financial Sector in Controlling Money Laundering

Global countermeasures have been arranged by the *Financial Action Task Force on Money Laundering* (FATF) as the Forty Recommendations in 1990 and revised in 1996. The majority of the Recommendations are about the 'role of the financial system in combating money laundering'[30] because of the effectiveness of the involvement of financial institutions in detecting money laundering (ML): Further, as Gilmore (1999: 83) noted, the more important factor was the awareness 'of the negative impact which "dirty money" can have on the credit and financial institutions through which it passes or in which it is deposited or invested in the course of laundering operations', though this 'awareness' amounts to an assertion rather than a demonstration of harm. Banks in the US spend from five to six percent of their compliance budget for AML and foreign asset control requirements.[31] Four important tasks are imposed upon banks and non-bank financial institutions of member countries.

1. 'Know Your Customer' (KYC) Requirement

Firstly, financial institutions have been required to know in order 'to identify, on the basis of an official or other reliable identifying document, and record the identity of their clients [. . .] when establishing business relations or conducting transactions'.[32] The policy is slightly enlarged in the UK as the Money Laundering Reporting Officer (MLRO), who is appointed by the financial institution, is requested to verify not only the KYC information but also the 'know [their] business information' (FSA 2001, Annex A: 17). However, the practical lengths to which institutions should go to 'know their customer' are variable: some jurisdictions[33] are required to identify the beneficial owners of accounts, whereas others[34] are not. KYC rules themselves should not be considered a burden because to comply with the rules benefits the industry as well.[35]

2. The Requirement to Retain Evidence

Having a close relation to the previous mentioned requirement, financial institutions are required to retain the data. The FATF requests to keep 'for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities'.[36] Retained data in this manner becomes evidence of internal audits (Gilmore 1999: 87), to say nothing of criminal prosecution by means of seizing.

3. Transaction Scrutinising Requirement

In addition, financial institutions should examine, with special attention, any transaction which they regard as particularly likely, by its nature, to be related to ML.

Although a majority of the FATF jurisdictions have adopted the system of self-vigilance of financial institutions, the US and Australia have applied a variation of this system. The latter system merely applies a 'fixed threshold' of transactions for triggering the reporting and thus financial institutions are not required to be cautious about the dubiousness of transactions (Gilmore 1999: 88).[37] Thus, compliance with this scheme may be easier than the former. In other words, Financial Intelligence Units, rather than the industry, fulfil the duties of identifying suspicious (in the professional criteria of crime control) transactions from massive amounts of data. Nevertheless, the development of counter-techniques should not be ignored.

4. Requirement of Suspicious Transaction Reports (STR)

The final requirement is to report the information of transactions that are suspected (or are over the threshold) to the Financial Intelligence Units (FIUs). Since reporting without firm criminal evidence may

30 Recommendations 8-29, FATF.
31 "Anti-money laundering rules among most expensive compliance cost for banks, ABA says". Money Laundering Alert, June 11 2003. http://www.moneylaundering.com/.
32 Recommendation 10, FATF.
33 Jurisdictions such as Guernsey and Jersey.
34 For example, Japan, the UK and US.
35 Dan McAleese argues that firms are naturally expected to know their customers in order 'to reduce counterparty risk' and 'to offer the best service to the customers'. See "KYC - a guide to the processes and techniques". Complinet, 5th June 2003. http://www.complinet.com/ml/dailynews/print_display.html?ref=46690.
36 Article 12, FATF.
37 Since then, they have introduced suspicious activity reporting to supplement routine reporting. See http://www.fincen.gov/reg_statutes.html.

give rise to conflicts with the interest of banking secrecy, the FATF suggests the need to exempt reporters from the liability to maintain confidentiality.

To summarise the impact of these requirements, it can be deduced that financial institutions have shared a considerable burden and responsibility for AML measures despite the fact that they are private businesses. The relationship between the financial sector and the authorities responsible for combating ML may be comparable to that of the telecoms industry and law enforcement agencies.

C. Analogical Points to the Counterpart

Thus, the relationship between policing and the financial sector is surveyed in this paper in parallel with that of the telecoms sector. The reason why these two issues are paired is that they are comparable. Three comparable points can be found as follows.

1. Increasing Universality in Relation to Crime

The first point is that both of these industries have a universal relationship to crime facilitation and inhibition, and, in both cases, the private sector has to be persuaded and compelled to assist in measures that are not automatically in its own short-term economic interests.

As the explanatory report of the Convention on Cybercrime points out -

> [technical] developments have given rise to unprecedented economic and social changes, but they also have a dark side: the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies. Moreover, the consequences of criminal behaviour can be more far-reaching than before because they are not restricted by geographical limitations or national boundaries.
>
> (Council of Europe 2001: para. 5)

Meanwhile, financial gain is the most important aspect of the majority of crimes. According to the PIU report around 70 percent of recorded crime in England and Wales is acquisitive (PIU 2000: para. 2.5). In addition, some non-acquisitive crime, most significantly terrorism, is only available when it is facilitated by underground money transactions. Johnson (2002) states that the definition of ML has changed after the terror attacks on the US. Whereas the term originally focused only on 'the criminal origin of what appears to be clean money', it is now re-defined and widely accepted as 'moving funds through financial institutions or accounts to disguise its origin *and/or purpose'* (Johnson 2002: 10, italics added). In fact, the Bush administration devised the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act. The Congress found that-

> money launderers subvert legitimate financial mechanisms and banking relationships by using them as protective cover for the movement of criminal proceeds and the financing of crime and terrorism[.][38]

The definition of money laundering in Japan has been enlarged by two steps. First, adopting the FATF Recommendations, the Punishment of Organised Crime and Control of Proceeds of Crime Law in 2000 defined it. The introduction was remarkable progress as the FATF evaluated that-

> the Japanese money laundering system in [June 1998], was not effective in practice[.] [. . .] The new Law extends the definition of money laundering to cover over 200 predicate offences.
>
> (FATF 2000, para. 95 and 96)

The second step was taken by the Punishment of Terrorism Financing Law in 2002. It was to create a type of criminal offence which punishes an act of financing for the purpose of committing terrorism, and then to make it a predicate offence for money laundering.

In this manner, financial policing has become increasingly significant and capable of wide application for criminal investigation, and thus it can be regarded as one of the primary investigative tools, like telecoms policing.

---

38 Section 302 (a) (3) of the USA PATRIOT Act.

2. Global Nature

Issues of facilitating financial policing are global matters in striving towards effective countermeasures for the global threat of trans-border crime, for example drugs dealing and international terrorism. Especially, the AML initiatives are even comparable with the issue of 'tackling global warming'[39] for insufficient measures by any responsible party may cause worldwide vulnerability. Since the beginning of the FATF, members have self-assessed and a mutual assessment scheme was added in 1992 (Gilmore 1999: 94). The latter might be observed as being a powerful method to harmonise policies among sovereign countries, although there is some risk of stigmatising 'rogue states' (Levi and Gilmore 2002: 361).

A similar situation can be found in the field of telecoms policing. Law enforcement capabilities have increasingly been vulnerable with the advance of technology and services. The international roaming function of mobile telephones, for example, offers criminals a more reliable and useful tool. On the Internet, the threat of an anonymous remailer controlling crime is aggravated by the existence of boundaries of jurisdiction. Generally, technologies and services are not defined domestically in the global age. Rather, the design of domestic facilities is bound by *de facto* standards designed by the oligopolistic manufacturers and the core technologies and system configurations are substantially based on international technical standards.

Another concern in a global context is the impact on the international competitiveness of businesses subject to compliance. A UK ex-investigator remarked that financial institutions in the UK are greatly handicapped in the European competitive market by the compliance burden of the AML provisions of the Terrorism Act 2000 and the Anti-terrorism and Security Act 2001 (Hamblin 2002). In this sense, offshore banking might be viewed as a threat to the domestic industry in common with law enforcement.

The identical concern in conjunction with lawful interception capabilities is expressed by Sutter (2001). He argues that due to the compliance burden of interception capabilities borne by RIPA, ISPs in the UK are at risk in the domestic market from international competitors located outside the jurisdiction of the UK who might provide cheaper services.

Again, it is summarised that telecoms policing is comparable with financial policing in the light of globalisation; in that both have been impacted negatively. However, unlike telecoms,[40] the reaction of financial policing, i.e. the AML movement, is backed by a fairly coherent global movement of key political institutions, such as the G7, OECD, UN, Council of Europe and EU, that has evolved over the past decade and a half (Gilmore 1999).

3. Compliance Costs

The compliance cost is also comparable. For the financial industry, AML compliance leads to a 'heavy burden' of paper work (Sheptycki 2000: 146). Especially, the examination of transactions would be mentally burdensome if the transaction were made, for example, by a 'good' customer. In addition, as a respondent to the FSA proposal of AML, particularly large-scale organisations might have the problem of an 'un-manageable' number of transactions to be examined (FSA 2001: 12). Even in the earliest stage of AML, KYC rules have been unwelcome. For example, British banks see the principle to be the 'high compliance costs, with little demonstrable benefit other than for anti-money laundering purposes' (FSA 2001: 10), although such outspoken complaints cannot be heard in the post 9/11 era.[41]

Similarly, it is known that various requirements, they are arguably burdensome, are assigned to the telecoms industry. However, unlike the impact of financial policing, there are few fact-finding enquiries into the burden of the industry except for the 'data retention' issues.

---

39 "Cleaning up dirty money", The Economist, 24th July 1997.

40 The only exception to this is the Convention on Cybercrime which obliges member states to adopt the procedural law on telecommunication policing.

41 Hamblin (2002) raises the question of jurisdictionally differentiated anti terror regulations in the aftermath of 9-11. Firms in countries that adopted draconian legislation would suffer 'a competitive disadvantage with firms from other countries', rather than the internal compliance cost of AML and anti-terrorism requirements.

V. DISCUSSION AND CONCLUSIONS

A. Theoretical Discussion on State vs. Non-state

1. Crime Control by the State and Private Sectors

By Max Weber's definition, the 'state' inevitably monopolises the legitimate enforcing powers (Weber 1947: 154). However, this classic paradigm was denied half a century later. Stanley Cohen (1985: 40-41) noticed that not only the state but also lay volunteers and professionals took measures in an overlapping manner to control deviance. The expansion of social control was conveniently justified by the state explaining that benign and professional players who have 'natural resources', rather than bloated 'overburdened, inefficient and inhumane' state systems, should be given the power (p.77). According to his metaphor, there are many fishers (parents, neighbours, teachers, social workers, probation officers, prison officers) setting their own nets to catch fish (offenders) in the sea (jurisdiction). Whereas the catches of the formal net (prison) are politically or fiscally controlled, the coverage of the nets of non-state fishers has widened or the nets have been changed into more finely woven ones to catch more fish (p. 41-42). In addition, 'there is far more room for the weaker form of privatization [than that of offender treatment apparatus] where the state contracts out certain services to private enterprise, retaining some measure of control' (p. 64).

Here, Cohen's *visions of social control* are reinforced. Various cases of telecoms policing examined in previous chapters fit exactly in his recognition by converting the *sea* from the real jurisdiction of the state to cyberspace. For, cyberspace is composed of private domains with public access, like rising mass-private property (p. 67), operated by the private telecoms industry. The same is equally true of financial policing, as Sheptycki (2000: 137) takes up the problem of the uncontrollability of 'electronic money [. . .] in cyberspace'.

Garland (1996) analysed the macro strategies on criminal control of the sovereign state. He began by identifying the limitation of the state's capability in controlling crime in the contemporary circumstances. He discovered the 'responsibilization' strategy adapted by the sovereign state. That is, the state has handed some roles of crime control, which had long been monopolised by the governmental agencies, over to non-governmental organisations and individuals. In this process, risks and costs incurred by crime have been distributed to the responsibilized private sector (p. 451).

The role of the state and non-state players in controlling *'Electronic Theft'* - type crime is examined by Grabosky et al. (2001). Due to the limitations of law and law enforcement, the state has responsibilized various parties to prevent cybercrime on the principle of potential victims' self-help. Based on the situation, they predict that technology will be primarily entrusted with the mission to control electronic theft, and that the state will have a mutually complementary relationship with industry for technological intervention (p. 206).

2. The Shortcomings of Responsibilization

Garland's criticism of responsibilization was that it might damage a balance of security level in its distribution distorted by the market principle. He (1996: 463) applied this idea in the real space focusing only on the dimension of the haves versus the have-nots. Upon reflection the dichotomy may be applied to the composition between the conventional telephone services operated by state-owned and/or mega-carriers vs. tiny ISPs who have the ethos of self-governance. The former would be more tolerant than the latter toward responsibilisation in complying with the state's request. Therefore, responsibilising in cyberspace might bring forth a disparity in crime control. Otherwise, an effective and fair cost sharing mechanism has to be devised. The same is true of responsibilizing financial policing measures. As the results of interviews suggest, banks have complied more loyally with AML requirements than non-banks and non-financial services have.

3. Charging the Compliance Costs to 'Those Who Benefit'

The discussion on the burden sharing of Situational Crime Prevention (SCP), the simple responsibilisation form of crime control (Garland 1996: 453), are two-fold. First, if the costs are 'modest', then the potential victim would pay the costs. The second approach is to invoice the costs to 'would-be' offenders. Namely, potential offenders should pay as beneficiaries because they are incapacitated from committing crime. These methods appear, at first glance, ethically unproblematic for they conform to the benefit principle (Duff and Marshall 2000: 23-24).

However, identifying 'those who benefit' is a complex issue. First, the major part of targeted crime for telecoms policing, e.g. drugs dealing,[42] victimises nobody or society on the whole. In the same way, there may be no other choice than determining that legitimate society is the victim of ML. In a sense, society has paid the policing costs through taxation and the state ought to compensate the industries. One might argue that the industries are the potential victims in an indirect manner because their integrity is at reputational risk[43] through crime facilitated by services provided by the industries. Even so, as far as such an intangible risk might be negligible, and the compliance costs would be, arguably, too much, the responsibilising strategy unavoidably seems to be not very effective.

However, the second option would be more problematic. Would-be offenders may be a subset of customers of the services at large. This logic might justify the diversion of compliance costs to all customers because differentiation between would-be offenders and the law abiding might be impossible and inappropriate. Based on this pessimistic analysis, all customers are equally treated as possible offenders and will receive bills. Thus, it is problematic and presumably ineffective if the beneficiary-payment principle alone is applied. In addition, since crime prevention is not the sole purpose and effect of telecoms and financial policing, stronger accountability is needed.

4. Boomerang Effect on the State

The next method is to return the fiscal responsibility to the state from the responsibilized party. Surprisingly, few theorists advocate this method for AML measures. However, for telecoms policing, it has already materialised in many jurisdictions. Inoue argues that the compliance costs of the telecoms industry in installing interception capabilities should be compensated by the state if the costs exceed a reasonable level (Inoue 1997: 212), though there may be arguments about what a 'reasonable level' is.[44] The notion might be influenced by the dogma that policing ought to be the monopolistic mission of the state. Either way, since the state is not a cornucopia; the costs are collected from taxpayers. In this case, the policing regime is reinforced because the paid industries are not only responsibilized but also obligated to comply.[45] Thus, moderating the compliance dilemma, the strategy might be welcomed by the non-state agencies. For, the concern of crime control being not a priority for them even though they are responsibilized, they would otherwise give profit making, for example, priority over responsibility.[46] The bottom line seems to be that the policy needs the backing from taxpayers consisting of haves and have-nots, netizens (network citizens) and non-netizens, criminals (provided that they pay tax, which is rare) and non-criminals.[47]

5. Para-taxation system: Responsibilizing cost recovery as well

At least in the traditional context, this state contribution strategy might be quite appropriate and be justified because the citizens are assumed to be the principal beneficiary of policing. Nevertheless, taking into consideration the history and the dynamism of industrial services, applying such a burden sharing approach to the responsibilization of financial and telecoms policing seems to be still unfair. Rather, the liable party would be the industry as they have an ethical responsibility, and the redirection of the costs to customers should be justified. Of course, the state, rather than responsibilized industry, continues to hold the primary responsibility for crime control. Consequently, the expenses being borne only by customers of responsibilized services may be equated with a kind of earmarked tax imposed on the customers by the industries.

B. Improving the AML Scheme

Responsibilizing the industry for financial policing is a good example of para-taxation.[48] In all interviewed

---

42 Japanese interception has never been applied to crime other than drugs related crime.

43 See case studies above on both Japanese and British mobile phone operators.

44 The notion may not always be applicable. For example, subsidising the *tachiainin* costs for the Interception Law might be problematic. Since watching the process is the role of the *tachiainin*, such compensation by the party to be watched might be viewed as the emasculation of the watchman. In addition, reimbursing might distort the market and create an entrance barrier to the business (APIG 2003: para. 176).

45 See Duff and Marshall (2000: 33) for the difference between responsibilities and obligations.

46 See Garland (1996: 464).

47 In addition, it is needed for taxpayers to approve the cases offering mutual legal assistance, for example, where beneficiaries of the system are citizens of other states on the reciprocity principle.

48 Having this conception, Sheptycki (2000: 165) predicts that the responsibilised financial institutions for a global AML system will become cogs in the global tax collection systems in the future.

countries and in Japan, AML costs are borne by responsibilized institutions and ultimately passed on to the customer. In order to ensure full cooperation with the industry it is recommended that they be informed of the significance of their compliance obligations. In fact all interviewees understand the burden on the industry of compliance, although none of them mentioned the conflicts with the industry.[49] In recognition of this burden some government agencies have taken steps to motivate the industry by, for example, liaising on a regular basis, issuing guidelines and giving feedback of information.

1. Interaction with the Industry

First, information sharing is the most universal tactic, as Johnston (1992: 192) pointed out. In order to facilitate STRs with intelligence value, good sanitised cases and negative examples are provided through web-sites or newsletters by every FIU. In addition, the Suspicious Transaction Report Office (STRO) in Singapore has regularly organised outreach programmes to discuss the STR scheme and obtain feedback. The STRO believes that these programmes contribute to a mutual understanding and build a close relationship with the industry. Similarly in Ireland, an interviewee pointed out how regular meetings with banks that are held twice a year and a bi-monthly steering committee with industrial representatives are important in establishing a good relationship.

2. Providing Guidelines

Almost all interviewees perceived the significance of supporting the industry by providing routine procedures to comply practically with the rules. Guidelines for AML compliance are issued by regulating authorities and industry organisations. Even where the government provides them, authorities welcome industrial participation to make them practical. In Britain, consultation papers for rules[50] and guidelines[51] have been circulated to incorporate opinions since before the first guidelines were published in 1990. In Hong Kong, the HKMA has published and updated the guideline entitled the 'Prevention of Money Laundering' since 1993. The draft guidelines and updates involved consultation with the industry. Coping with recent developments of FATF recommendations after the 9/11 event, and the issuance of the paper 'Customer Due Diligence for Banks' by the Basel Committee on Banking Supervision, the 'Supplement to the Guideline on Prevention of Money Laundering' was drafted in consultation with banks. Many questions and comments submitted to clarify the requirement in a practical context are quite helpful to establish a feasible system. Through the consultation process, these guidelines have become the product of the co-operative work.

3. Feedback Systems for STRs

The feedback systems for STRs in two jurisdictions are remarkable. The GBFI in Ireland is obliged to give feedback on the status of investigation to the reported institution every six months until the content of the feedback becomes 'no further action'. A MLRO of a bank set a high valuation on the system, not only because the two-way communication is crucial to mutual understanding. Rather, the information is useful to improve the internal reporting system by providing sanitised good and bad cases as materials in annual training classes and newsletters for bank staff.

Similarly in Singapore, the police are responsible for giving feedback for emergency telephone calls and complaints within six months in order to maintain the service level, and the feedback system for STRs was established by improving this system. The STRO is responsible for giving notice to those who lodge a STR, whether the police will proceed with the case or not, within fourteen days.

By contrast, the CTIF-CFI in Belgium is prohibited by law from providing information to reporters. FIUs and law enforcement agencies in Hong Kong and the UK are in between these two cases; i.e. they sometimes provide feedback. However, no feedback is given for the majority of reports. A current issue that has arisen in the UK is how to improve the communications between the industry and law enforcement agencies.

---

49 A British interviewee referred to the estimate by the think-tank KPMG that calculated the total compliance costs for all the British banks at ninety million pounds per year.
50 Issued by the FSA.
51 Issued by the British Banker's Association, Association of British Insurers, etc.

Without doubt, feedback would be welcomed by the complying party in general and might increase overall performance of the AML system. Are not compulsory feedback systems feasible in other jurisdictions? One reason why the larger jurisdictions like the UK (67,000 STRs in 2002) and Japan (18,768 STRs) do not apply such systems may be that responding within a certain period of time is not feasible, unlike in smaller jurisdictions like Ireland (4,398 STRs) and Singapore. The organisational structure might be another factor, e.g. the FIU and the user of financial intelligence are separated or many agencies use the intelligence.[52] As the Belgian system prohibits disclosing the confidentiality of investigations, the sensitive nature of investigative information can be another reason for hesitating to disclose information.

However, the author thinks a compulsory feedback system should be introduced to larger jurisdictions rather - because they are more complicated and thus require more transparency. As far as the information is sensitive, the FIU may maintain confidentiality by just informing the complying party that the case is ongoing. Granted that the majority of feedback messages will state that it is ongoing, and no further information will be provided for a long period because of limited human resources and organisational arrangements, for example in the UK and Japan; such a situation would be far better than having no feedback at all.

In the UK, there are 50,000 backlogged STRs to be processed and even if some reports are distributed 'to the local police forces, there is very often nobody there to deal with them'.[53] If there has been no active investigation of an STR for a long time, it may be assumed that the value of the STR has decreased.[54] As in many other policing spheres, criticism may be needed to improve systems and the absence of open criticism may merely reflect the absence of evaluation rather than that systems are working well. Thus, the feedback system might place FIUs and law enforcement agencies under surveillance. If there is no (or poor) feedback because of the insufficiency of investigative resources, then the heaviness of the industrial burden cannot be justified. Therefore, the government has to allocate resources proportional to the compliance costs of the industry rather than calling for ever more STRs.

C. Reasonable Burden Sharing for Telecoms Policing

1. Subsidising Telecoms Policing

In summing up the interviews - policies for the subsidisation of telecoms policing may be categorised into three types. (1) The first option is to compensate the initial compliance costs. The arrangement in the UK for installing interception capabilities[55] and for retaining data[56] falls under this. (2) The second one is to subsidise in exchange for fruits of the initial compliance. The Belgian subsidy scheme for 'usage fees of interception capabilities' and 'the purchase of retained data' epitomise this method. The US applied a similar reimbursement system for interception capabilities.[57] The governmental standards of 'pay-per-use' disbursements for (only operational) costs are always defined irrelevantly to the actual costs incurred initially by the industry and may be disproportionately low to the latter. However, paying only corresponding sums of usage might be more rational, at least for the states, than pre-paying. Because, in adopting the pre-payment scheme, it would be extremely difficult to determine the installation costs of interception capabilities and data retention functions integrated into sophisticated network systems without affecting the domestic free competition market. (3) Finally, if the government does not subsidise at all, the industry would face the 'price of doing business'.[58] The same applies to the Japanese policy on interception capabilities provided that the costs are reasonably low.[59] Both in Ireland and in Japan, not complying with the requirement of capabilities is not illegal. However, unlike in Japan, the conditional licensing policy of Belgium guarantees that the industry will comply.

---

52 Both criteria are applied to Japan and the UK.

53 "A few tips about suspicious transaction reports". Complinet, 23rd April 2003.
http://www.complinet.com/ml/dailynews/print_display.html?ref=45552.

54 Of course, there is some possibility of having later 'hits' on the same individual or on intermediaries working with him/her. Nevertheless, the chronic delay in processing might spoil the secondary effect as well.

55 Section 14 of RIPA.

56 Section 106 of ATCS.

57 See AOUSC (2003: 11).

58 See APIG (2003: para. 144).

59 Again, the definition of 'reasonableness' comes into question.

If the burden of financial policing is settled by adopting para-taxation systems after all, then the tactics might be applicable to telecoms policing in general as well without resort to the regulatory powers. Because, the author does notice internet-widening rather than net-widening. The para-taxation systems can be justified for several reasons.

2. Justifications for the Para-taxation Systems

First, unlike the condition of real world policing, there was neither a crime opportunity nor a victim in cyberspace. Thus, policing powers were not necessary at all. The balance was lost when the 'new social space'[60] was created. Although major telecoms services were state owned (e.g. the Japanese telephone network)[61] or monopolised for research purposes (the Internet) in the beginning; unfortunately the crime opportunity was facilitated with the earliest forms of cyberspace. Both the opportunity and victimisation of crime has increased since then. Second, presumably the customers of telecoms policing, i.e. criminals, are unevenly distributed among the customers of the telecoms service who pay for the services as well as state tax, than non-customers who pay tax only. Further, within the community of netizens, the more the netizens pay for the services, presumably the more criminal opportunities would be available for them. Almost the same applies to the distribution of potential victims. Third, the trans-border nature of crime facilitated by telecoms services 'is in conflict with the territoriality of national law enforcement authorities' (Council of Europe 2001: para. 8). Although the capabilities and experience of state-funded policing has increased, on the one hand, such policing practices might threaten the sovereignty of foreign countries (see Sheptycki 2000: 161), and on the other, they would be less accountable to domestic taxpayers than domestic policing. Thus, diverting the costs for policing in cyberspace to netizens would be justified by the fact that the costs of real-space policing are supported by the state's tax-collection from citizens under the jurisdiction.

Thus, the netizens would naturally shoulder the costs of counter-crime mobilised in cyberspace just as citizens do for crime in real space. The author does not mean that the industry caused criminals to commit crime. On the contrary, it is evident through the studies in previous chapters that they have been always willing to defend their integrity.[62] However, they have unfortunately faced two fundamental limits. The telecoms industry should, on the one hand, provide a universal service (Hayashi and Tagawa 1994), and, on the other, comply with the constitutional request to keep confidentiality of telecommunications, the freedom of expression and the ban on censorship.[63] In other words, the industry had been *incapacitated from contributing to controlling crime.* From this perspective, the responsibilization process is serving the remedial purposes by immunising as long as it is appropriately grounded.

3. Feasible Steps Forward

Nevertheless, such a utilitarian solution would not work if adopted aggressively. First, though involvement should be limited being beyond the scope of this paper, concerns of citizen or *netizen* rights should be settled by establishing appropriate due process systems. In addition, such a cost-redirection policy would arouse the hostility of smaller sized or new entrant service providers and benign customers. More substantially, the issues of international competitiveness of the domestic industry should be taken into consideration. Providing that the responsibilizing degrees are unbalanced, customers of domestic services are vulnerable to differentiated (1) redirected costs, (2) degrees of inconvenience, and (3) at least Orwellian unpleasant feelings. By the nature of cyberspace, sensitive customers with sufficient motivation would migrate from nuisance domestic services to 'offshore' (APIG 2003: para. 159) or elsewhere. In addition, there is no reason for would-be offenders to hesitate to do so (para. 162). Thus, there is the danger of both the 'hollowing out' of the industry and the negative effect of the displacement of crime. In effect, the strategy might ironically cause damage to the national interests.

After all, domestic responsibilization policies without due consideration would not be advisable. Rather, the solution should be facilitating the international harmonisation of (1) the extent and the justification of diverting costs to customers, and (2) the extent of telecoms policing capabilities, i.e. the potential degree of

60 See Manning (2000).
61 The service was privatised in 1985 (Hayashi and Tagawa 1994: 216).
62 The reason why the industry was often reluctant to comply would be the weak justification of diverting costs, the Orwellian concerns of reputation and the anxiety of losing competitiveness. As subsequently discussed, these spells should be broken.
63 Article 21 of the Constitution, for example in Japan.

restriction on human rights. There may be at least two approaches to harmonise the disparities of domestic conditions.

First, law enforcement agencies as well as regulatory agencies of telecommunications need to organise a collective policy on policing needs and regulating telecoms services. The Convention on Cybercrime is a monumental first step. In addition, there are comparable forerunning projects. The feasibility of the responsibilization policy is proven by AML movements. As FATF have powerfully tackled problems of inter-jurisdictional ML, establishing, for example, a Telecoms Action Task Force (TATF) or some other body for the resolution of the *inter-net* issues of telecoms policing might be worth considering. The agenda of the TATF would resemble that of the *FATF*. The main issue may be how to distribute costs and functions of telecoms policing among those jurisdictions that i) are the hosts of the hub of an international network; ii) have intense competition; or iii) provide offshore services. Some existing practical problems in conducting mutual legal assistance might be naturally resolved through these discussions. However, the author does not advocate establishing only the TATF, because such a top-down solution might be less accountable for the time being than the approach discussed below.

Second, the most recommended approach would be to facilitate the standardisation of *technology* (see Grabosky et al. 2001: 206). Because, all components of cyberspace are microscopically interconnected in only a technical dimension, by neither market pressure nor political dynamism nor law, as Lessig (1999: 207) puts it, 'code is law'. Through the sober standardisation process, a technically rational system design would be obtained. Thus, the friction arising from introducing telecoms policing measures might be smoothened if it conforms to legitimate technical standards. A part of the standardisation effort in conjunction with lawful interception capabilities has already been established by the ETSI. The standardisation may not necessarily be bound within the purely technical sphere. As ISO 9000 and 14000 series[64] standardised not purely technical matters but managerial, the standards of telecoms policing may treat security matters in a wider sense. The 'security-related function' may contain functions of surveillance, incapacitating criminals, the removal of illegal contents, the retention of data for the access of law enforcement, etc. The functions of the internationally average level of due processes should be embedded with policing functions. Above all, the standardisation processes should be operated in an open and democratic way. All stakeholders, e.g. not only the service providers and manufacturers, but also representatives of customers, human rights advocates and law enforcement agencies, should have access to the process. Especially, law enforcement officials have to take the trouble to persuade by explaining the significance of telecoms policing capabilities. At the same time, governments would be well advised to ensure that the costs of cybercrime control do not become an impediment to the creative and productive use of digital technology.

The author neither assumes such a prescription to be the Utopia nor advocates realising the Orwellian surveillance society. The absence of police, surveillance, control and responsibilization is the largest happiness of the greatest number provided that there is no crime or victim. Rather, we, who enjoy the current prosperity and convenience brought forth by telecommunication and financial services, should duly be responsibilized to solve the difficult problems derived from the utility.

64 http://www.iso.ch/.

REFERENCES

Andrews, S. (2002) *Privacy & Human Rights*: An International Survey of Privacy Laws and Developments. Washington, DC: Electronic Privacy Information Center. Retrieved 31st December, 2002 at http://www.privacyinternational.org/survey/phr2002/.

AOUSC (Administrative Office of the United States Courts). (2003) *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications* (2002 Wiretap Report). Washington DC: Administrative Office of the United States Courts.

APIG (The All Party Internet Group). (2003) *Communications Data: Report of an Inquiry by the All Party Internet Group.* London: APIG. Retrieved 21th March 2003, at http://www.apig.org.uk/APIGreport.pdf.

Banisar, D. (2000) *Privacy & Human Rights*: An International Survey of Privacy Laws and Developments. Washington, DC: Electronic Privacy Information Center.

Clarke, R.V. (1997) Part 1: Introduction. In: Clarke, R.V. (Ed.) *Situational Crime Prevention*: Successful Case Studies (2nd edition). New York: Harrow and Heston Publishers.

Cohen, S. (1985) *Visions of Social Control.* Cambridge: Polity Press.

Council of Europe. (2001) *Convention on Cybercrime: Explanatory Report.* Retrieved 5th January, 2002 at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

Council of the European Union, The. (1996) Council Resolution of 17 January 1995 on the lawful interception of telecommunication: Official Journal C 329, 4th November 1996. pp. 0001-0006. Retrieved 3rd January, 2003 at http://europa.eu.int/smartapi/cgi/
sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=41996Y1104(01).

Denning, D.E. and Baugh, W.E. Jr. (1997) Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism. Washington DC: National Strategy Information Center.

Diffie, W. and Landau, S. (1999) Privacy on the Line: The Politics of Wiretapping and Encryption. Cambridge (Massachusetts), London: The MIT Press.

Duff, R.A. and Marshall, S.E. (2000) Benefits, burdens and responsibilities: some ethical dimensions of situational crime prevention. In: Hirsch, A.V., Garland, D. and Wakefield, A. (Eds.) Ethical and Social Perspectives on Situational Crime Prevention. Oxford: Hart Publishing.

FATF (Financial Action Task Force). (2000) Financial Action Task Force on Money Laundering: Annual Report 1999- 2000. Paris: FATF Secretariat. Retrieved 5th May, 2002 at
http://www.orlingrabbe. com/fatf_ar_2000.pdf.

FSA (Financial Services Authority). (2001) *Money Laundering: The FSA's New Role:* Policy statement on consultation and decisions on rules. London: The Financial Services Authority.

Garland, D. (1996) The limits of the sovereign state: Strategies of crime control in contemporary society. *British Journal of Criminology,* Volume 36, Number 4, pp. 445- 471.

Gilmore, W.C. (1999) *Dirty Money: The Evolution of Money Laundering Countermeasures,* (Second Edition). Strasbourg: Council of Europe Publishing.

Grabosky, P.N. and Smith R.G. (1998) *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities.* Leichhardt, NSW: The Federation Press.

Grabosky, P.N., Smith R.G. and Dempsey, G. (2001) *Electronic Theft: Unlawful Acquisition in Cyberspace.* Cambridge: Cambridge University Press.

Hamblin, C. (2002) The UK's terrorist legislation: a risk manager's warning. *Complinet* (Money Laundering), 11 March 2002. Retrieved 23rd December, 2002 at http://www.complinet.com/ml/dailynews/print_display.html?ref=33044.

Harrington, V. and Mayhew, P. (2001) *Mobile Phone Theft,* Home Office Research Study 235. London: Home Office.

Hayashi, K. and Tagawa, Y. (1994) Universal Service: the principle of 'fairness' in the multimedia age. Tokyo: Chuko Shinsho.

Homusho (Ministry of Justice, Japan). (1998) *Hanzai Sosa no tameno Tsushin Boju ni Kansuru Horitsu An Kankei Shiryo* (Reference Data for 'Bill of Telecommunication Interception for Criminal Investigation'). Tokyo: Homusho.

Inoue, M. (1997) *Sosa Shudan to shiteno Tsushin/Kaiwa no Boju* (Telecommunications' Interception and Eavesdropping as Investigative Tools). Tokyo: Yuhikaku.

Johnson, J. (2002) 11th September, 2001: Will it make a difference to the global anti-money laundering movement? *Journal of Money Laundering Control,* Volume. 6, Number 1, pp. 9-16.

Johnston, L. (1992) *The Rebirth of Private Policing.* London: Routledge.

Keisatsucho (National Police Agency, NPA). (1996) Heisei 8 Nen Keisatsu Hakusho (White Paper on Police 1996). Tokyo: Keisatsucho.

Keisatsucho. (1999) Heisei 11 Nen Keisatsu Hakusho (White Paper on Police 1999). Tokyo: Keisatsucho.

Keisatsucho. (2000) Explanatory Notes to Punishment of Organised Crime and Control of Proceeds of Crime Law. Tokyo: Keisatsucho.

Lessig, L. (1999) Code and Other Laws of Cyberspace. New York: Basic Books.

Levi, M. and Gilmore, B. (2002) Terrorist finance, money laundering and the rise and rise of mutual evaluation: a new paradigm for crime control? European Journal of Law Reform. Volume 4, Issue 2, pp. 337-364.

Lloyd, I. J. (2000) Information Technology Law (third edition). London: Butterworths.

Manning, P.K. (2000) Policing new social spaces. In: Sheptycki, J.W.E. (Ed.) Issues in Transnational Policing. London: Routledge.

Mostyn, M.M. (2000) The need for regulating anonymous remailers. *International Review of Law Computers & Technology,* Volume 14 (1), pp. 79- 88.

PIU (Performance and Innovation Unit). (2000) *Recovering the Proceeds of Crime.* (A PIU Report). London: Cabinet Office. Retrieved 21st March 2002, at http://www. cabinet-office.gov.uk/innovation/2000/crime/recovering/contents.htm.

Sheptycki, J. (2000) Policing the virtual launderette: Money laundering and global governance. In: Sheptycki, J.W.E. (Ed.) *Issues in Transnational Policing.* London: Routledge.

Sutter, G. (2001) A tale of two interception regimes: RIP v CALEA, a comparison. *16th BILETA Annual Conference* (April 9th - 10th, 2001). Retrieved 30th December 2002, at http://www.bileta.ac.uk/01papers/sutter.html.

Thomas, P.A. (2002) Legislative responses to terrorism. In: Scraton, P. (Ed.) *Beyond September 11: An Anthology of Dissent.* London: Pluto Press.

Tsuchiya, T. (2001) Digital jidai no gohoteki tsushin boju Europe hen (Lawful interception in the digital age - Europe issue). Chijo, November, pp. 14-20. Retrieved 6th May 2003 at http://www.glocom.ac.jp/project/chijo/2001_11/2001_11.pdf.

Weber, M. (1947) *The Theory of Social and Economic Organization* (Translated by A.M. Henderson and Talcott Parsons, Edited with an Introduction by Talcott Parsons). New York: Oxford University Press, New York.

WISTA (World Information Technology and Services Alliance). (2000) World Information Technology and Services Alliance (WISTA) Statement on the Council of Europe Draft Convention on Cyber-crime. Retrieved 26th December 2002, at http://www.witsa.org/ papers/COEstmt.pdf.