- *for the defence of justification to succeed, the disclosure may have to be to the "proper authorities" only.*

This last requirement is probably the least satisfactory from the media's point of view. In cases of alleged wrongdoing, for example, the only permissible disclosure may be to the police. Similarly, in cases involving medical danger, the "proper authority" may be public health officials rather than the general public.

Judicial Hostility

It may be argued that Australian courts should follow the example of their more liberal English counterparts in weighing the importance of a free press in the context of public interest debates in confidentiality cases. Such moves would, of course, be counter to the popular notion of protecting the individual's limited 'rights' of privacy in a media-intrusive age. It may also require a reversal of the judiciary's distrust of the media which is at times thinly disguised. The comments of Justice Powell in the *Westpac Letters* case about the "self righteous" media are telling:

"In vigorously arguing for the public's "need to know" and in whipping up public opinion on the matter, they tend to create an environment in which confidentiality becomes much harder to maintain, thereby assisting the case against restraint. However, it is hardly surprising if this creates judicial hostility: judges who feel as if they are being backed into a corner.... will only be human if their reaction is a stiffened resolve to show that they cannot be dictated to by the media."

Jason Macarthur is a lawyer with Tress Cocks & Maddox in the Sydney office. The views expressed in this article are those of the author and not necessarily those of the firm.

International Electronic Money Systems and Money Laundering

Brent Fisse and Peter Leonard examine net-smurfing and other emerging regulatory challenges from electronic payment technologies.

Much has been said about the increasingly global social problem of money laundering and the potential ways in which this problem might be minimised. The advent of electronic payment technologies (**"EPT"**) raises several important questions of regulatory approach and design which have tended to fall between the cracks in the current debate, including the following:

- *EPT are diverse and, although* electronic in operation, are likely to be much more difficult to bring within a common centralised financial transaction reporting system than the relatively homogeneous and concentrated banking system which has been the focus of Australia's significant financial transaction and international wire transfer reporting scheme to date. The trend is towards automating suspect transaction reporting. The rise of EPT service providers raises the question of what can be done to spur the development of such smart systems generally.

- Structured transactions (**"smurfing"**) are a pandemic way of evading the significant financial transaction and international wire transfer reporting obligations under the Financial Transaction Reports Act 1988 (Cth) (**"Act"**) but the present regulatory controls under s 31 of that Act are vague and unworkable. The use of structured transactions will be facilitated by EPT, as in the context of Internet-based smurfing transactions (**"net-smurfing"**) where transaction costs are low and the opportunities for automating structured transactions are high. What practical solutions, if any, are there to this intractable problem?

- AUSTRAC has successfully persuaded at least the major banks to co-operate extensively in gathering and supplying significant financial transaction and international wire transfer information in a format readily usable by AUSTRAC's computer-based screening systems. Is it plausible to suppose that the same "softly, softly" approach will work with EPT operators at least some of whom will be aggressive new entrants with little or no loyalty to the traditions of mainstream Australian retail banking? If not, consideration needs to be given to other regulatory strategies including a statutory "pyramid of enforcement" capable of dealing effectively with non-compliant as well as compliant entities and their staff.

- Developing effective technologies for reporting or searching for relevant intelligence conveyed by means of EPT is likely to impose significant capital and recurrent costs on those who do have to install and operate the systems necessary for reporting and/or searching.

Suspect Transaction Reporting

EPT are diverse and, although electronic in operation, are likely to be much more difficult to bring within a common centralised financial transaction reporting system than the relatively homogeneous and concentrated banking system which has been the focus of Australia's significant financial transaction and international wire transfer reporting scheme to date. The trend is towards automating suspect transaction reporting. The rise of EPT service providers raises the question of what can be done to spur the development of such smart systems by banks and EFT service providers.

There is much disenchantment with suspect transaction reporting regimes, for several reasons. First, it is difficult to distinguish between objectively suspect transactions and those which, short of the threshold, are merely suspected. Secondly, the suspect transaction test is

narrower than that of "unusual" transactions and may easily exclude useful intelligence. Unusual transactions may provide critical investigative linkages, which partly explains why FATF Recommendation 15 envisages that financial institutions will keep a watch out for "unusual" patterns of transactions.

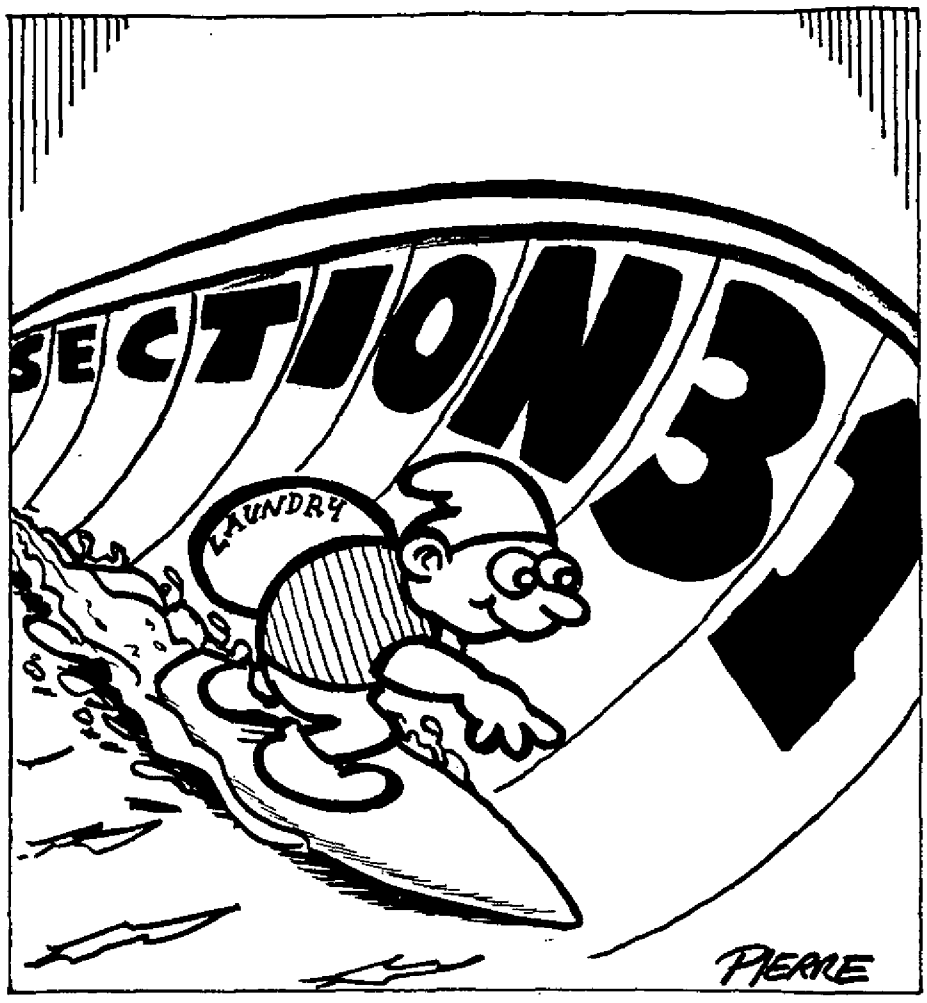
Thirdly, an empirical study by Michael Levi of suspect transaction reporting in the UK[1] indicated a very low strike-rate - around one *arrest* of a suspected drug trafficker per 200 suspect transaction reports. Fourthly, the sheer number of transactions handled by most financial institutions means that any checking of particular transactions is likely to be cursory and quite possibly unreliable.

More fundamentally, suspect transaction reporting based on human suspicion is increasingly outmoded in a world where there are very large numbers of routine electronic banking transactions.

The whole idea of a suspicion-based system is old-fashioned, since unlike burglaries and robberies, most cross-border transactions are conducted purely electronically, without anyone physically seeing them: because of the legislation (and sometimes to guarantee that the transaction will be paid for) customers must be identified, but how are bankers to know whether there is a legitimate "business case" for the myriad of transactions they undertake, and why should it be their business to "shadow" their customers? Legislation does not require them to do those things, but they (and the "informal banking" sector) would have to do so if they were to smoke out all the laundering and fraud.[2]

The more automated the banking and financial system becomes, the less face-to-face contact between clients and employees and the greater the holes in the detection net unless client information is electronically scanned for abnormal patterns and connections. This growing reality has already been recognised in Australia in the context of significant cash transactions reports and details of all wire transfers - the data is automatically sent by the banks to AUSTRAC for checking and the checking process involves a variety of pattern matching and other computer-based detection routines.[3]

AUSTRAC has moved towards relying more on suspect transaction reporting based on the automated collection of objective data rather than reliance on the subjective human judgment of tellers and



their supervisors. Shortly it is planned that computerised programs within banks may generate Suspect Transaction Reports, at least in relation to certain rudimentary indicators of possible money laundering. This project (called autoSUSR) will help to deal with some of the criticisms by law enforcement agencies that certain rudimentary behaviour is not reported.[4]

Given this trend towards automated suspect transaction reporting, the growth of EPT service providers may well impel further development of smart systems.

One approach would be to fast track the development of smart reporting systems technology for EPT service providers and other financial institutions by AUSTRAC and to amend s 17 of the Act so as to give EPT service providers and other financial institutions the right to opt out of the standard suspect transaction reporting requirements where they enter into an enforceable undertaking with AUSTRAC to develop and install a smart system compatible with AUSTRAC reporting protocols and which alone or in combination with human oversight procedures is approved by AUSTRAC as a system reasonably capable of achieving the reporting of unusual transactions.

This is an adaptation of the enforced self-regulation approach advanced by John Braithwaite in the context of suspect transaction reporting by banks. The model of enforced self-regulation envisaged by Braithwaite would require financial institutions to spell out the particular way in which they would go about detecting suspect transactions and ensuring that staff acted according to that plan.[5]

Whether or not there are sufficient incentives for EPT service providers to take the enforced self-regulation route is another question. A "softly, softly" approach may be seem insufficient (see section 4 below). Another key issue is who is to pay for the costs of developing smart systems.

The Problems with Smurfing Offences Under Section 31

The recent decision of the high Court in *Leask v the Commonwealth*[6] that s 31 of the Act is within consitutional power does not address the concerns raised at the outset of this article about the evasion of

reporting obligations under the Act by means of structures transactions.

Internal controls by financial institutions against structured transactions work on the basis of checks for cash deposits by a customer which in aggregate exceed the threshold amount at which a single cash transaction must be reported. One major difficulty is to indicate to financial institutions the time-frame within which they are obliged to aggregate deposits without also letting smurfs know what adjustments they need to make to avoid getting caught by the aggregation tests. As explained below, this problem arises under the anti-smurfing provisions under the Act.

The smurfing offences under s 31 of the Act are defined essentially in terms of the test whether, given the nature of the transactions, it is "reasonable to conclude" that a dominant purpose of the transactions was to evade the reporting obligations under the Act. The test under s 31 is not related to any given period during which financial institutions are expected to aggregate transactions involving a particular customer. There is no specific obligation under the Act to aggregate deposits or other cash transactions. Instead, "the aggregated value of transactions" is one of the indicia (see s 31(1)(b)(I)(B)) which the trier of fact is to consider when applying the "reasonable to conclude" test.

The *ex post facto* nature of the test of liability under s 31 puts banks and other financial institutions in a precarious or impossible position. The "reasonable to conclude" test implies that financial institutions are under an obligation to aggregate cash transactions yet they are not in a position to know what exactly that obligation requires of them at the time when the transactions take place. Worse, the test is not applied until the matter is determined by the trier of fact. Financial institutions thus remain under an obligation to aggregate deposits until such time as the matter is decided in a prosecution or civil proceeding. So open-ended an obligation to aggregate is not merely vaguely defined but impractical. To comply with it, conceivably a bank would need to aggregate deposits on a perpetually rolling basis, perhaps for years after an initial transaction took place. If the legislation does not require banks to go to such extreme lengths, where is the line to be drawn?

It is also unclear whether the required standard of compliance is the same across the wide variety of organizations and bodies subject to s 31, or whether it varies depending on the technology available to the particular organization. What exactly are banks and other financial service providers supposed to do to keep track of deposits or other transactions at their various branches? A major interstate or international bank may have a sophisticated computer network which makes the task of aggregation a relatively simple one, whereas a small finance company or on-line service provider may lack any corresponding facility.

If, for example, a bank has a computer-based tracking capability that enables it instantaneously to aggregate all deposits made at any branch within, say a 24-hour period, then it may well be "reasonable to conclude" on the basis of the information available to that bank that the sole or dominant purpose of the customer was to evade the reporting requirements. On the other hand, if a bank does not have such a computer-based capacity, perhaps it is unreasonable to arrive at the same conclusion.

Section 31 does not resolve the most critical question here, which is whether or not banks and EPT service providers are expected to install systems that will enable aggregation of deposits made at all branches or for all machines dispensing smart cards, instantaneously or within say a daily or other period. Many financial institutions in Australia as elsewhere do not presently have the capacity to aggregate deposits at all branches even on a daily basis. If they are expected to acquire some greater capacity, it seems harsh to make them run the gauntlet of an ill-defined penal provision. Moreover, installing adequate systems takes time and systems cannot sensibly be installed until it is known what exactly the expected standards of aggregation are. The same applies to the emerging EPT industry and the planning that needs to go into their hardware and software requirements.

Possible Solutions

One possible solution would be a system, developed in conjunction with the banking and finance and EPT industries, under which different aggregation periods are used by different financial institutions at different periods arranged on a secret roster basis.[7] Financial institutions would then know exactly where they stand, yet smurfs would not be presented with aggregation rules which could easily be circumvented. Such a system supposes that banks and other financial institutions have the technical capability to alter the time settings of their aggregation programs periodically at low cost. It also assumes that the roster arrangements could in fact be kept secret from the smurfing underworld.

Another possible approach is via enforced self-regulation, with each bank or EPT service provider determining its own aggregation rules - smurfs would not be faced with a standard aggregation period which could easily be circumvented but with many unknown and different aggregation periods[8]. This approach assumes that the aggregation period selected by a given bank could in fact be kept secret from smurfs. It does not necessarily assume a technological capacity to change the aggregation periods periodically at low cost. However, such a capacity might well be essential to reduce the risk of disclosure.

The only approach which seems to be capable of avoiding the otherwise high risk of the aggregation periods being leaked to smurfs is a centrally controlled system under which aggregation periods for each and every financial institution are selected randomly by a computer program and then transmitted and deployed in such a way that no human agent has access to the random sequence. Utopian?

A further hurdle to aggregation is the possibility that transactions could be structured across a number of institutions (i.e. using digital cash from a number of different issuers) as well as by breaking the total value of such transactions into smaller sums.[9] Inter-bank aggregation of transactions would present substantial practical difficulties, in addition to further privacy issues.

"Softly, Softly" Regulation, or Negotiation and Settlement Within a Statutory Pyramid of Enforcement?

A luminous feature of AUSTRAC's record is its success in persuading at least the major banks to co-operate extensively in gathering and supplying significant financial transaction and international wire transfer information in a format readily usable by AUSTRAC's computer-based screening systems.

Whether the same spirit of co-operation is likely to be attainable in the context of EPT service providers is another question. At least some will be new entrants committed to developing their

businesses at low cost may balk at incurring the expenditure which may be needed to introduce significant transaction and international funds transfer funds reporting systems which are compatible with AUSTRAC's data handling systems. Not all will agree with the merits of being subjected to the reporting obligations imposed under the Act or the wisdom of voluntary co-operation for the sake of community interest.

Consistently with the objective of achieving co-operation and consensus as far as possible, and assuming that EPT service providers are or will be regulated under the Act, consideration needs to be given to strengthening the Act so as to enable AUSTRAC and other enforcement agencies to help bring any non-compliant EPT service providers and other "new wave" financial institutions into line.

AUSTRAC has indicated its wish to have additional civil remedies to strengthen its hand.[10] The design of any such amendments is best approached from the broader perspective of a "pyramid of enforcement" strategy capable of dealing with non-compliance with remedies and sanctions of whatever severity and type required to bring about compliance and mutual co-operation.[11] Such a strategy, which would require some amendments to the Act is already a well-known feature of ACCC enforcement policy and practice (it is less apparent on the part of the ASC, which has been criticised to some extent for failing to adopt a sufficiently explicit policy for the settlement of enforcement actions).

Who will Bear the Enforcement-related Cost of new EPT Reporting and/or Searching Requirements?

Developing effective technologies for reporting or searching for relevant intelligence conveyed by means of EPT is likely to impose significant capital and recurrent costs on those who do have to install and operate the systems necessary for reporting and/or searching. Australian banks, like their US counterparts, have generally taken the costs on the chin in the past, but this seems largely a quirk of history. It is significant that carriers successfully objected to the "enforcement agency user does not pay" principle which surfaced under the draft 1997 telecommunications legislation in the context of interception under the *Telecommunications (Interception) Act* (Cth) but which was later abandoned in the *Telecommunications Act* 1997 (see s 314). EPT service providers should be quick to make the same point if attempts are made to enlist them as unpaid deputies to fight money laundering.

It is far from obvious why the social cost of providing interception capability or monitoring capability should be imposed on financial institutions rather than spread more through general taxes as in relation to the costs of improving stolen vehicle tracking systems or enhancing surveillance technology for detecting terrorists or plane hijackers. EPT service providers and other financial institutions should hold out for the user pays principle and rely on the model provided by s 314 of the *Telecommunications Act*.

Conclusion – Balance or Bust?

Michael Levi has observed of regulatory controls against money laundering that:

> *"[t]he trick of regulation is to minimise the illegitimate exploitation without wrecking the economic dynamism"*[12]

The regulatory challenges canvassed in this paper intensify rather than reduce what is already a difficult balance.

1 Levi, *"The Reporting of Suspicious Money-Laundering Transactions"* (1994))

2 Michael Levi, "Money Laundering and Regulatory Policies" in "Savona" ed. *"Responding to Money Laundering: International Perspectives"* Amsterdam: Harwood Academic, 1997 at 279.

3 See AUSTRAC, *AUSTRAC Papers 1992.*

4 AUSTRAC, *The Next Phase* (1995) 14.

5 Braithwaite, *"Following the Money Trail to What Destination?"* (1993) 44 Alabama Law Review 657, 665.

6 Unreported, 1996.

7 Fisse, Fraser and Coss, eds, *The Money Trail*, Sydney: Law Book Co., 1992 at 186.

8 Braithwaite, *"Following the Money Trail to What Destination?"* op cit. at [ ]

9 Tyree *Digital Cash* Sydney: Butterworths, 1997 at 4.89.

10 AUSTRAC, *The Next Phase* (1995) 22-23.

11 See further Ayres and Braithwaite, *"Responsive Regulation"* New York: Oxford University Press, 1993.

12 Levi, *"Money Laundering and Regulatory Policies"* op cit. at 260.

Brent Fisse and Peter Leonard are partners with Gilbert and Tobin.