



The Prosperity Institute

August 30, 2002

Financial Action Task Force on Money Laundering
Secretariat
2, rue André Pascal
75775 Paris Cedex 16
France

Dear Sir or Madam:

This letter is submitted for the purpose of commenting on the Consultation Paper dated May 30, 2002 issued by the Financial Action Task Force on Money Laundering (FATF). The comments herein are based primarily on research and deliberations conducted by the Task Force on Information Exchange and Financial Privacy. The initial findings of the Task Force were published in May 2002 in its Report on Financial Privacy, Law Enforcement and Terrorism. A copy of the entire report is attached in PDF format and is available at <http://www.prosperity-institute.org/projects/PI-TF-Report.pdf>. We request that this report be made a part of the record.

The Task Force on Information Exchange and Financial Privacy was formed in July, 2001 under the auspices of the Prosperity Institute to systematically research and analyze information exchange laws, organizations, mechanisms and proposals and their implications for financial privacy and economic prosperity. The Task Force developed specific proposals that meet the legitimate needs of the national security and law enforcement communities and the reasonable requirements of tax administration while respecting privacy, including financial privacy. It was composed of former senior U.S. government officials (including law enforcement officials), economists, attorneys and privacy experts who approach the project from a wide variety of perspectives.

The recommendations in the report offer a means of both substantially increasing the effectiveness of efforts to combat terrorism and crime and improving the degree to which the privacy of law-abiding citizens is respected. Most notably, the members of the Task Force unanimously determined that the best means of ensuring a balance of needs is not to take the approach adopted by the FATF in requiring ever more information from parties involved in financial transactions. Rather, we resolved that there must be an international convention that

establishes minimum benchmarks for financial privacy, and sets forth the duties and obligations of governments that can be trusted with that information.

The Consultation Paper is extremely disappointing because it demonstrates unwillingness on the part of FATF:

- to place any appreciable value on the privacy and civil liberties of individuals;
- to acknowledge the vital, even life-saving, importance of financial privacy to some people and organizations throughout the world;
- to establish serious restrictions on the use to which governments and others can put to information obtained by virtue of FATF's efforts;
- to genuinely prioritize terrorism and the exchange of information about terrorists;
- to establish serious restrictions on which governments and individuals can obtain sensitive information obtained by virtue of FATF's efforts;
- to place any appreciable weight on the cost of the increasingly complex and intricate rules being implemented, particularly in small countries or on small businesses;
- to establish metrics by which the effectiveness (or lack thereof) of various rules can be measured;
- to establish accountability for FATF and its staff; and
- to consider the economic implications of its proposals and their impact on the standard of living of the public.

Privacy and Civil Liberties

There has been nothing but perfunctory acknowledgement by FATF of the importance of privacy, including financial privacy, and civil liberties.

Financial privacy can be the difference between an opposition group in a country governed by a dictator surviving or being systematically tortured or assassinated. Financial privacy can prevent kidnappers from identifying profitable targets. Financial privacy can help prevent corrupt officials from abusing their trust. Financial privacy is the instrument citizens can use to protect themselves from corrupt or criminal influences. Financial privacy can allow people to protect their life savings when a government confiscates its citizens wealth, whether for political, ethnic or other reasons. Financial privacy can be the difference between a business failing or succeeding. Financial privacy, in short, is of deep and abiding importance to the improvement of the human condition because many, perhaps most, governments have shown themselves capable of routinely abusing private financial information.

FATF has not set forth standards regarding what information should and should not be shared or obtained in connection with its Recommendations (as is common in treaties on taking evidence abroad). FATF has no apparent standards regarding governments or individuals with whom information should not be shared. FATF appears to have no policies, procedure, sanctions or concerns relating to the protection of information being abused once it has been shared between governments or agencies. FATF appears to believe (see, e.g., paragraph 184) that information obtained ostensibly for law enforcement purposes should be eligible for use by governments for any purpose (regulatory, tax, civil, etc.).

In our view, restrictions must be placed on the information that can be obtained and shared by government and privacy deserves more consideration than the occasional token acknowledgement that there may be such a thing as “legitimate” privacy, because the very purpose of law enforcement is to protect the blessings of a free society – and one such blessing has been the acknowledged right to privacy.

FATF should devote some of its considerable resources to developing such standards.¹ Our recommendation is that democratic countries adopt the Convention on Privacy and Information Exchange set forth in Appendix B of this letter. This Convention would establish minimum standards in international law and make them enforceable. At the very least, the standards set forth in the draft convention should serve as a guide to FATF and become part of the Recommendations.

Turning lawyers, accountants, real estate agents, jewelry stores, car dealers and others into a network of spies (see Section 5, Non-financial Businesses and Professions, paragraphs 226-298), will increase the size of the informational haystack, and involuntarily conscript more and more members of society as informers. Where will FATF's recommendations stop? It seems that FATF is moving toward the UN High Level Panel on Financing for Development position that every government should know everything about everyone on the planet. We find such an Orwellian prospect unacceptable. A free society depends on a separation of the roles of the police and the citizenry. And most governments do not adequately respect human rights and cannot be expected to treat such information appropriately.

The proposal to impose on attorneys the legal duty to breach attorney client privilege shows the lengths to which FATF is currently willing to go (paragraph. 272 et seq.). Attorneys are currently under an obligation to disclose evidence with respect to future crimes. That is sufficient. To go further would constitute a substantial blow to our system of justice, making effective assistance of counsel extraordinarily difficult by chilling legitimate legal inquiry and limiting the right of accused to defense.

The Appropriate Use of Information

It has become apparent that the current international framework for information sharing is inadequate to achieve the needs of law enforcement and national security. This is true of FATF, Interpol, the EU and U.S. efforts (most notably FinCEN). Although the current system is extremely good at collecting large amounts of information on law abiding citizens, it is of extremely limited value in actually combating crime or terrorism because there is so much useless information being collected and because the means are not in place for the secure sharing of useful information among interested parties in law enforcement and intelligence in different governments.

We believe that routine, secure information sharing among democratic countries is appropriate for national security, anti-terrorism and law enforcement purposes provided that the appropriate

¹ In other words, the perfunctory “strict safeguards” language in Recommendation 32 needs to be given real substance.

security and due process protections are in place. We believe that the priority should be national security, anti-terrorism and law enforcement.

The Task Force recommends that democratic countries enter into a Convention on Privacy and Information Exchange (1) to make information exchange for national security, anti-terrorism and law enforcement purposes more effective, (2) to prevent the information obtained and shared from falling into hostile hands, and (3) to protect, in a legally enforceable manner, the privacy of innocent persons.

The activities of the Convention's adherents should be limited to obtaining and sharing information for national security, law enforcement and anti-terrorism purposes. The Convention should develop and enforce protocols to ensure the information is not provided to hostile parties or used for inappropriate commercial or political purposes or for other purposes unrelated to law enforcement or anti-terrorism efforts. Protocols should ensure that private information of innocent persons is protected and that such information is not provided to anyone other than government personnel in law enforcement or national security functions. The Convention should provide a private right of action for persons in member states to enforce their legal rights under the Convention in member state courts. The principal of double criminality should be honored, such that, an act or omission should be a crime in all member states to be the subject of information sharing. Currently FATF does not promote any such protections.

The Security of Information

FATF has expressed support for using Interpol (see Recommendation 31) as a means of exchanging information. Indeed Interpol recently established a database for purposes of sharing information about terrorism. This database will be made available to all Interpol members. Interpol includes countries known to sponsor terrorism (e.g. Iran, Iraq, Libya, Somalia, Syria, Sudan), other countries that may be hostile to the West (e.g. the People's Republic of China, Cuba, Yugoslavia) and countries with major corruption problems (e.g. Bulgaria, Colombia, Nigeria). Financial Action Task Force members (particularly its regional and observer status participants) also pose unacceptable security risks.

Accordingly, no existing international organization, as currently constituted, has both the breadth to be effective and the standards to ensure that the national security of democratic states and the privacy of their citizens are protected. It is impossible for FATF or Interpol to serve as a genuine clearing house for information since the security threat posed by member countries is simply too high. A system that does not allow the U.S. and its allies to freely exchange relevant information will not be effective in preventing terrorism or enhancing Western national security. The FATF and Interpol systems are so inclusive and free of meaningful restrictions that it would not be prudent to provide full information to these databases for fear that some government or some official in a corrupt or potentially hostile government will use the information to thwart the anti-terrorism or national security purposes of the database. A more restrictive arrangement is absolutely necessary in order for the project to work effectively.

There is the need to restrict the information shared to national security, law enforcement and anti-terrorism purposes. These restrictions are even important in the case of friendly

governments to ensure that the information is not used for inappropriate purposes (e.g. commercial, political, tax administration or civil purposes). Only by imposing these restrictions will participants' confidence in the system be high enough that they will freely provide information. There is the need to make these restrictions legally enforceable and to monitor that they are being honored in practice in the same way FATF now envisions monitoring compliance with its information exchange requirements.

The Task Force believes that by establishing a new Privacy and Information Exchange Convention subject to meaningful, enforceable restrictions on membership and the use to which information can be put can the kind of free exchange of information necessary to effectively combat terrorism be facilitated. The new convention would internationalize traditional liberal legal principles such as protections against unreasonable search and seizures and due process of law. It would provide for enforceable restrictions on the use to which information can be put and provide persons within adhering states a private right of action to enforce the Convention.

With changing technologies, ever-higher standards for information and data integrity must be recognized. Any information system can be compromised. It is important to recognize that it is easier to compromise a system from within. Data needs to be protected from natural disasters or accidents (requiring backup, distribution, redundancy), human error and input problems (concerning verification and validation), and unauthorized access (constantly examining access control and security with an eye toward deterrence, traceability and investigative preparation).

Cost-Benefit and Metrics

FATF has exhibited almost no concern for the costs being imposed on the private sector by its increasingly complex and intricate regulatory system. It has made no attempt to measure or assess those costs. Perhaps more fundamentally, it has not established or recommended metrics about how to measure the effectiveness of its recommended policies. FATF's core philosophy is simply more information means more effectiveness. Besides ignoring the cost to the private sector and the cost to taxpayers, this is demonstrably false. Burying law enforcement in even more useless paper will not increase their effectiveness. FATF must seriously evaluate the effectiveness of its manifold recommended rules, regulations and policies before its puts in place even more. The effectiveness or lack thereof in assisting law enforcement needs to be compared to both the financial costs imposed on the private sector and the intangible cost in terms of lost privacy.

Paragraph 15 of the Consultation Paper specifically sets forth the general considerations that FATF will weigh, including, "the costs and benefits that arise in relation to particular measures." This invitation is a good start. FATF should not delegate the important task of analyzing costs and benefits to the public, but itself should publish a thorough cost benefit analysis for review on each of the recommendations.

A procedural parallel in this consideration is Office of Management and Budget (OMB) Circular No. A-94, which in combination with the due process protections under the U.S. Administrative Procedure Act mandates Federal agencies perform such an analysis. OMB Cir. A-94 states that "benefit-cost analysis is recommended as the technique to use in a formal economic analysis of

government programs or projects." Through it agencies try to determine whether a government program can be justified on economic principles, i.e. whether the monetized value of expected net benefits greatly exceed costs. Net present value is computed by assigning monetary values to benefits and costs, discounting future benefits and costs using an appropriate discount rate, and subtracting the sum total of discounted costs from the sum total of discounted benefits. Although net present value is not always computable (and it does not usually reflect effects on income distribution), efforts to measure it can produce useful insights. For example, has FATF considered the costs of providing sensitive information in to FATF member nations, such as the members of the Gulf Cooperation Council or governments involved in observer status groups. Is the possibility that the information will be used against FATF member nations a cost? If so, what is that cost? Has FATF considered how much these rules will cost business? What types of businesses? Consistent with the OMB Circular, FATF's analyses should be explicit about the underlying assumptions used to arrive at estimates of future benefits and costs. Key data and results, such as year-by-year estimates of benefits and costs, should be reported to promote independent analysis and review.

A comprehensive enumeration of the different types of benefits monetized or not, can be helpful in identifying the full range of effects of FATF framework. Rather than doing any of this, FATF simply implies that the standards are of some benefit in fighting crime or terrorism without elaboration. Of what benefit? How quantified? Quantifying benefits and costs is worthwhile, even when it is not feasible to assign monetary values. Examples include the number of terrorist attacks avoided, or fraud schemes uncovered.

FATF has claimed that its measures are "widely accepted" and "successfully implemented." However, while some nations have been strong-armed into accepting them, have they been successful in their desired effect? Retrospective studies to determine whether anticipated benefits and costs have been realized are potentially valuable. Such studies can be used to determine necessary corrections in existing programs, and to improve future estimates of benefits and costs in these programs or related ones. Quite simply, FATF should have a plan for periodic, results-oriented evaluation of program effectiveness. They should also discuss the results of relevant evaluation studies when proposing these changes.

Finally, the FATF should incorporate in its analysis proper consideration of the effects on small entities. A parallel here is the U.S. Regulatory Flexibility Act, 5 U.S.C. 601 et seq. When U.S. agencies promulgate rules - indeed, rules which are much less sweeping effect than those considered by FATF here - they strive to thoroughly review draft rules to assess and take appropriate account of the potential impact on small businesses, small governmental jurisdictions, and small organizations, as provided by the Act. Through this means, the U.S. seeks to ensure that the spirit of rules can best be accommodated in the least costly and intrusive way.

Existing money laundering rules in the United States currently generate so many "suspicious activity reports" (156,000 in 2000) and "currency transaction reports"(12,000,000 in 2000) that reports about the activities of criminals and terrorists are lost in a mountain of useless reports about citizens going about their law-abiding activities. The Currency Transaction Report system is particularly ineffective because of the sheer volume of reports generated and because the

system is so simple to evade by even moderately sophisticated criminals. Suspicious Activity Reports are problematic because of the necessary lack of clear and objective guidelines. Unfortunately, the U.S. Congress just made the situation worse with the passage of the USA PATRIOT Act which further expands the reporting system and, in effect, increases the size of the haystack which the law enforcement community must search for the terrorist and criminal “needle.”²

The last thing that would be constructive in the effort to apprehend terrorists and criminals would be to generate even more untargeted reports by, as has been proposed, reducing the reporting threshold or broadening the reporting network. To rationalize the effort to apprehend terrorists and criminals, the current CTR and SAR system should be replaced. Instead, the authorities should generate a confidential “watch list” consisting of individuals and organizations (and their known aliases, identifying numbers and addresses) about which there is reasonable and significant suspicion of involvement in terrorism, other threats to national security or serious crimes.

Accordingly, the proposed option 2 in paragraph 140 requiring “reasonable grounds to suspect” represents an improvement.

A mechanism should be established whereby governments can employ computer technology to compare this watch list with the accounts maintained in financial institutions in the U.S. and abroad (by means of the proposed Privacy and Information Exchange Convention and otherwise) and if a match is made, the government would obtain a report of the financial transactions involving the accounts in question.

To effect such a system, financial institutions and government would need to cooperate to establish high legal standards and practices, and systems that allow an automated matching of the financial institution account databases and the watch list database. The matching program should examine names, identifying numbers and addresses.

Since some terrorists organizations have used financial fraud to finance their activities, increased attention to information integrity and systems security, including improved personnel training, could help prevent incidences of identity fraud and other problems. FinCen and other financial regulators should encourage the adoption of better data security and encrypted e-mail and other communications.

Accountability

In the "Introduction" FATF stated that member countries will have implementation monitored through "an on-site examination." Presumably, this means that entities and individuals subjected

² The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (which includes the *International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001*, the *First Responders Assistance Act*, the *Crimes Against Charitable Americans Act of 2001*, and the *Critical Infrastructures Protection Act of 2001*) (H.R. 3162; Public Law No: 107-56).

to FATF's framework, such as lawyers, banks and mutual funds, may be subject to investigation by FATF members, to determine whether they have successfully implanted the FATF recommendations. FATF is quite willing to use draconian sanctions against governments that do not toe to its line. One option in paragraph 259 for regulation and supervision real estate agents is to have oversight by "one or more designated competent authorities." The emphasis on oversight and sanctions is evident throughout the report

However, there is one important body that FATF left out of the oversight requirements - itself. It is ironic, that FATF does not allow for any similar on-side evaluation or even self assessment of the most important part of the framework: an evaluation of the success of the very initiatives required of FATF. Even if they did, they have developed no established metrics for determining the success versus the costs of its proposals.

More importantly, it is not clear what legal authority FATF has or who has practical legal authority or oversight capability over FATF. It is largely unaccountable to anyone or any institution. The question 'Who Oversees FATF?' remains to be answered. Certainly, there is the need for greater transparency and accountability at FATF.

Economic Implications

More and more complex and intricate regulations imposed on banks, insurance companies, securities firms, casinos, lawyers, accountants, car dealers and a host of other businesses have real economic costs running to the tens of billions of dollars per year or more. They distort markets and stifle innovation. They reduce economic growth and prosperity. FATF, however, shows no sign of recognizing the adverse economic effects of these costs as even a factor in its deliberations.

Another example of the lack of concern about the economic implications of its proposals, its FATF's hostility to potentially revolutionary technologies. The report purposes that electronic/purses/cards be tightly restricted. See paragraphs 71 et seq. The proposed restrictions include: limits on any single transactions; prohibitions on customer-to-customer transaction; linking purses/cards to a dedicated account; allowing only merchants to debit purses/card where purchases are made; not allowing purses/cards to be recharged; and requiring the system to record all transactions leaving an investigatory trail. These recommendations are contrary to good public policy on two fundamental grounds. First, it is desirable to encourage people to substitute electronic currency for physical currency (paper and coin), and the FATF proposals would do just the opposite. A substantial portion of all crime occurs when criminals attempt to seize someone else's physical currency. Using electronic currency greatly reduces the ability of criminals to steal money, and hence the use of electronic money will substantially reduce crime. Furthermore, electronic money is far less costly to move, store, and protect than physical money, and is also cleaner and more sanitary. However, despite these advantages people have and will be reluctant to use electronic money unless they are provided with the same degree of anonymity and freedom they enjoy with paper currency. The FATF proposal totally ignores the privacy rights of individuals. Second, the FATF proposal indicates that the authors seem not to understand the state of development of the science of electronic money creation and transmission. New developments in hardware, software, and encryption will make it easier and

easier for users of electronic money like products to move money outside the banking system instantaneously in anonymous fashion whether the authorities legally allow it or not. It is generally not wise to make something illegal that can be relatively easily done without detection, unless overwhelming public harm would occur by making it legal. In the case of electronic money/purses/cards/cellphones, etc. the case for unrestricted use is far stronger than the case for limitations.

We recommend that FATF withdraw its Consultation Paper and start over with these recommendations in mind.

Sincerely,

David R. Burton
Executive Director
Task Force on Information Exchange and Financial Privacy

Appendix A

Members of the Task Force on Information Exchange and Financial Privacy

Chairman

Hon. Mack F. Mattingly

Senior Advisors

Hon. Jack F. Kemp

Hon. Edwin Meese, III, Esq.

Executive Director

David R. Burton, Esq.

Members

Dr. Veronique de Rugy (Cato Institute)

Stephen J. Entin (Institute for Research on the Economics of Taxation)

James W. Harper, Esq. (PolicyCounsel.com, Privacilla.org)

Dr. Lawrence A. Hunter (Empower America)

J. Bradley Jansen (Free Congress Foundation)

Dan Mastromarco, Esq. (Prosperity Institute, Argus Group)

Dr. Daniel Mitchell (Heritage Foundation)

Andrew Quinlan (Center for Freedom and Prosperity)

Dr. Richard W. Rahn (Discovery Institute)

Solveig Singleton, Esq. (Competitive Enterprise Institute)

Mark A. A. Warner, Esq. (Hughes, Hubbard & Reed)

Hon. John Yoder, Esq. (Burch and Cronauer)

Appendix B

Convention on Privacy and Information Exchange

General Explanation

The current patchwork of international information exchange treaties, organizations and networks has two important flaws. First, the current system is not nearly as effective as it could and should be in aiding law enforcement and anti-terrorism efforts. Second, it imposes little or no legally cognizable restrictions on the use to which governments can put the information obtained and insufficiently protects individuals' privacy rights.

The proposed Convention would address both problems by making the international information exchange system much more effective and, for the first time, legally commit leading countries to the respect of individual privacy and provide enforceable restrictions on the use to which obtained information can be put.

The Convention would facilitate the exchange of information among Member States for national security, anti-terrorism and law enforcement purposes and only these purposes. In stark contrast to present practice, the Convention would establish legally enforceable rules to ensure this information is adequately protected and to prevent that information from being obtained by hostile parties, potentially hostile parties, parties that do not have adequate safeguards under domestic law or parties that in practice do not observe those safeguards. It would ensure that the information is not used for inappropriate commercial, political or other purposes.

The Convention would establish a private right of action, enforceable in Member State courts, with respect to the legal rights afforded to individuals under the Convention.

Convention on Privacy and Information Exchange

PREAMBLE

Whereas, the individual right to life, to liberty and to possess property are fundamental human rights and governments have an obligation to protect these rights;

Whereas, to better protect these rights, there is a need for greater cooperation among democratic states to obtain information and to facilitate the exchange of information for national security, law enforcement and anti-terrorism purposes;

Whereas, there is a need to protect individual privacy under international law;

Whereas, there is a need to ensure that sensitive private, national security, law enforcement and terrorism-related information is safeguarded,

Therefore, the States party to this Convention have agreed as follows:

Article I

ESTABLISHMENT OF CONVENTION

The Contracting States undertake to respect and to ensure respect for the present Convention on Privacy and Information Exchange in all circumstances.

Article II

PURPOSE

The purpose of this Convention shall be:

- (1) to facilitate the exchange of information among Member States for national security purposes;
- (2) to facilitate the exchange of information among Member States to detect, prevent or defend against terrorism and to apprehend persons who have committed acts of terrorism;
- (3) to facilitate the exchange of information among Member States to detect, prevent or defend against serious ordinary law crimes and to apprehend persons who have committed serious ordinary law crimes;
- (4) to protect the privacy of citizens of Member States and other innocent persons;
- (5) to ensure that information obtained by Member States or exchanged among the Member States by means of the Convention is adequately protected and to prevent that information from being obtained by hostile parties, potentially hostile parties, parties that do not have adequate safeguards under domestic law or parties that in practice do not observe those safeguards;

- (6) to ensure that information obtained by Member States or exchanged among the Member States by means of the Convention is used solely for purposes set forth in subparts (1) through (3) of this Article; and
- (7) to ensure that information obtained by Member States or exchanged among the Member States by means of the Convention is not used for inappropriate commercial, political or other purposes.

Article III

PRINCIPLES

The Member States reaffirm the following principles:

- (1) The right to life, to liberty and to possess property are fundamental human rights;
- (2) The governments of the Member States have an obligation to protect the national security of the Member States and to protect the lives, liberty and property of the citizens of the Member States from attack from hostile parties;
- (3) The governments of the Member States have an obligation to detect, prevent or defend against terrorism and to apprehend persons who have committed or planned acts of terrorism;
- (4) The governments of the Member States have an obligation to detect, prevent or defend against serious ordinary law crimes and to apprehend persons who have committed serious ordinary law crimes;
- (5) The governments of the Member States have an obligation to respect and protect the privacy of citizens of Member States and other innocent persons.

The Convention shall be guided by these principles.

Article IV

DEFINITIONS

For purposes of this Convention the following terms shall be defined as follows.

- (1) *Establishment* means any private:
 - (a) place of employment,
 - (b) office,
 - (c) place of assembly, or
 - (d) house of worship.
- (2) *National Security Purposes* means action reasonably calculated to detect, prevent or defend against:
 - (a) an attack by a hostile state or other hostile party on the territory of a Member State resulting in the loss of life or destruction of property;

- (b) an attack by a hostile state or other hostile party on the civilian or military personnel of a Member State government without the territory of a Member State;
 - (c) an attack by a hostile state or other hostile party on the citizens of a Member State without the territory of a Member State;
 - (d) an attack by a hostile state or other hostile party on the information systems infrastructure of a Member State; and
 - (e) espionage directed against a Member State or citizens of a Member State.
- (3) *Party or Parties* means one or more international organizations, states, belligerents, private entities, individuals or other organization, entity or institution and their respective agents, employees, personnel, citizens or residents.
- (4) *Person* means a natural person, a corporation, a private business entity or a private non governmental organization.
- (5) *Protected Person* means any person that is a national of a Member State, a lawful resident of a Member State or domiciled in a Member State.
- (6) *Serious Ordinary Law Crime* means conduct that (a) constitutes an offence in all Member States and (b) is punishable by a maximum deprivation of liberty of four years or more in all Member States.
- (7) *Terrorism* means (a) any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act, or (b) an act which constitutes an offence within the scope of and as defined in one of the following treaties:
1. Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970.
 2. Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971.
 3. Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973.
 4. International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979.
 5. Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980.
 6. Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988.
 7. Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988.

8. Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10 March 1988.
9. International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997.

Article V

MEMBERSHIP

- (1) The Contracting States shall be Members of the Convention, subject to this Article.
- (2) Each Member State is obligated to:
 - (a) maintain a democratic form of government;
 - (b) maintain adequate domestic laws against corruption in government;
 - (c) maintain adequate domestic law protecting individuals against deprivation of life, liberty or property without due process of law;
 - (d) maintain adequate domestic anti-terrorism laws;
 - (e) maintain domestic law that allows for the extradition of persons to other Member States that stand accused of committing or conspiring to commit under the law of another Member State one or more acts of terrorism or one or more serious ordinary law crimes;
 - (f) maintain domestic law that complies with Article VIII of this Convention relating to privacy;
 - (g) maintain domestic law such that Article IX of this Convention is enforceable;
 - (h) consistently and reliably comply in practice with the provisions of the Member State's domestic law referenced in this subpart (2);
 - (i) be a party to a treaty or treaties that, with respect to other Member States, provides for adequate mutual legal assistance in criminal matters; and
 - (j) consistently and reliably comply in practice with this Convention.
- (3) The Members of the Convention may decide to invite any Government prepared to assume the obligations of membership to accede to this Convention. Such decisions shall be unanimous. Accession shall take effect upon the deposit of an instrument of accession with the depositary Government.
- (4) Members of the Convention shall monitor the compliance or lack thereof of each Member with subpart (2) of this article. The Convention shall terminate the membership of any Member in the Convention that it finds is not in substantial compliance with subpart (2) of this article. Said termination shall be effective immediately upon the affirmative finding of two-thirds of the Members of the Convention at a meeting of the Convention and the terminated Member shall have no more standing in the Convention than any other non-member state. The terminated Member may be readmitted pursuant to subpart (3) of this article.

Article VI

GOVERNANCE

- (1) Unless the Members of the Convention otherwise agree unanimously for special cases, decisions shall be taken and recommendations shall be made by mutual agreement of all the Members.
- (2) Each Member shall have one vote. If a Member abstains from voting on a decision or recommendation, such abstention shall not invalidate the decision or recommendation, which shall be applicable to the other Members but not to the abstaining Member.
- (3) No decision shall be binding on any Member until it has complied with the requirements of its own constitutional procedures. The other Members may agree that such a decision shall apply provisionally to them.
- (4) A Convention Conference, to which all the Members shall be invited to send delegates, shall be the body from which all acts of the Convention derive. Each Member State shall designate a person or persons to participate in the Convention as delegates. Conference. Each Member shall have one vote in the Convention Conference. There shall be an annual Convention Conference. Special Convention Conferences may be called upon the request of a majority of the members. Each Member shall be responsible for its own expenses. Convention Conference expenses shall be borne by the host government.
- (5) Members shall designate each year a Chairman, who shall preside at its session, and a Vice-Chairman.
- (6) Members may establish an Executive Committee and such subsidiary bodies as may be required for the achievement of the aims of the Convention.
- (7) Upon such terms and conditions as the Conference may determine, the Convention may:
 - (a) address communications to non-member States or organizations;
 - (b) address communications to individuals or private institutions;
 - (c) establish and maintain relations with non-member States or organizations; and
 - (d) invite non-member Governments or organizations to assist in activities of the Convention.
- (8) The first annual Convention Conference shall be in . The time and place of subsequent Convention Conferences shall be as determined by the Members.
- (9) Each year, the Chairman of the Convention Conference shall issue a report describing and analyzing the operation of the Convention. The report may also contain recommendations of the Convention Conference. The Chairman shall make the report publicly available, provided however, that the Members may vote to not disclose a portion of the report if it determines that doing so is reasonably necessary to further the purposes of the Convention.

Article VII

GENERAL OBLIGATIONS

In order to achieve the purposes set forth in Article II, the Members of the Convention and those acting under their authority, in a manner consistent with this Convention and subject to the restrictions of this Convention, may:

- (1) obtain information,
- (2) provide information to other Member governments,

- (3) cooperate with law enforcement, intelligence and defense authorities of other Member governments,
- (4) make recommendations to other Members, and
- (5) enter into agreements with other Members, non-member States and international organizations.

In order to achieve the purposes set forth in Article II, the Members, in a manner consistent with this Convention and subject to the restrictions of this Convention, shall:

- (1) cooperate with law enforcement, intelligence and defense authorities of other Member governments,
- (2) enact and maintain domestic law to enforce Article VIII of this Convention, and
- (3) take steps to ensure that information obtained by means of the Convention and provided to other Members is safeguarded.

Article VIII

PRIVACY

- (1) No information obtained by means of the Convention shall be provided to any Member government and no Member government shall use information obtained by said Member government by means of the Convention except for the following purposes:
 - (a) for national security purposes,
 - (b) to detect, prevent or defend against terrorism and to apprehend persons who have committed acts of terrorism,
 - (c) to detect, prevent or defend against serious ordinary law crimes and to apprehend persons who have committed serious ordinary law crimes.
- (2) All Member Governments shall enact and maintain domestic law to enforce subpart (1) of this Article. Each Member shall ensure that individuals who act in contravention to subpart (1) of this Article shall be criminally liable such that said individual is (a) subject to deprivation of liberty of not less than four years, and (b) subject to dismissal if employed by the Member's government.
- (3) All Member Governments shall ensure that information obtained by means of the Convention or exchanged among the Member States by means of the Convention is not used for commercial, or political or other purposes unrelated to achieving the purposes of the Convention set forth in subparts (1), (2) and (3) of Article II.
- (4) Each Member Government shall respect the right of other Member Governments to respect and protect the privacy of citizens or other innocent persons in cases unrelated to achieving the purposes of the Convention set forth in subparts (1), (2) and (3) of Article II.

- (5) All Member Governments shall ensure that citizens of the Member States shall be secure in their persons, houses, establishments, papers and effects against unreasonable searches and seizures.
- (6) All Member Governments shall enact or maintain domestic law establishing adequate safeguards for the privacy of the citizens of the Member States. Said domestic law shall provide at least the following safeguards:
 - (a) protect individuals and private establishments from warrantless searches and seizures and require that warrants not be issued but upon a showing of probable or reasonable cause;
 - (b) prohibit the disclosure of tax information about individuals or private establishments obtained by Member States to private parties and restrict its use to national security, law enforcement, anti-terrorism or tax administration purposes;
 - (c) prohibit the disclosure of financial or personal information about individuals or private establishments that is (1) obtained by Member States by operation of law and (2) not in the public domain to private parties and restrict its use to national security, law enforcement, anti-terrorism or tax administration purposes;
 - (d) such other safeguards as the Members may provide, subject to the provisions of this Convention.

Article IX

RIGHTS OF PROTECTED PERSONS

- (1) Evidence obtained by a Member State by means of the Convention in deprivation of any rights, privileges, or immunities secured by this Convention, or other evidence obtained because of said evidence, shall not be admissible in a Court of Law of any Member State in a proceeding against a Protected Person or in an administrative proceeding of any Member State against a Protected Person.
- (2) Every person who, under color of any treaty, statute, ordinance, regulation, custom, or usage, of any Member State subjects, or causes to be subjected, any Protected Person to the deprivation of any rights, privileges, or immunities secured by this Convention, shall be liable to the injured Protected Person in an action at law, suit in equity, or other proper proceeding for redress.
- (3) To protect any rights, privileges, or immunities secured by this Convention, a Protected Person shall be entitled to injunctive relief in a Court of Law of competent jurisdiction of any Member State against:
 - (a) any Member State, or
 - (b) any person who under color of any treaty, statute, ordinance, regulation, custom, or usage, of any Member State,

who subjects, or causes to be subjected, said Protected Person to deprivation of any rights, privileges, or immunities secured by this Convention.

- (4) Each Member State shall take such steps as are necessary under its domestic law to ensure that Protected Persons' rights under this Article are secured.

Article X

RATIFICATION

- (1) This Convention shall be ratified or accepted by the Signatories in accordance with their respective constitutional requirements.
- (2) Instruments of ratification or acceptance shall be deposited with the Government of the United States, hereby designated as depositary Government.
- (3) This Convention shall come into force on 30th September, 2003, if by that date three Signatories or more have deposited such instruments as regards those Signatories; and thereafter as regards any other Signatory upon the deposit of its instrument of ratification or acceptance.
- (4) Upon the receipt of any instrument of ratification, acceptance or accession, or of any notice of termination, the depositary Government shall give notice thereof to all the Contracting States and to the Secretary-General of the Organization.

Article XI

TERMINATION

Any Member State may terminate the application of this Convention to itself by giving three months' notice to that effect to the depositary Government.

IN WITNESS WHEREOF, the undersigned Plenipotentiaries, duly empowered, have appended their signatures to this Convention.