



WITSA STATEMENT

Government and Law Enforcement Access to Transmitted Information In the Digital Environment August, 1998

INTRODUCTION

In the era of voice telephony, there was general agreement around the world that governments and law enforcement agencies could have legal access to telephone conversations for legitimate security and law enforcement activities. This principle is now being questioned, however, as the world is becoming increasingly digitized, and access to transmitted information includes not only voice telephony, but also data and video information. The tendency simply to extend voice telephony access to other media is becoming increasingly problematic to the business community in the global environment.

The health and prosperity of the information services industry is closely aligned with the degree to which business uses networks in its day-to-day business operations. Business must have confidence in the security and reliability of these networks for it to continue to place its sensitive business information on them.

This paper examines WITSA's understanding of the concerns of business in the hope that this will facilitate movement toward an international solution involving governments, the global law enforcement community and business. In addition, a set of Business-User Principles is set forth as a starting point for future discussion.

WITSA

Standard Background information on WITSA

The World Information Technology and Services Alliance (WITSA) is a consortium of 32 information technology (IT) industry associations from economies around the world (list attached). As the global voice of the IT industry, WITSA is dedicated to:

- advocating policies that advance the industry's growth and development;
- facilitating international trade and investment in IT products and services;
- strengthening WITSA's national industry associations through the sharing of knowledge, experience, and critical information;
- providing members with a vast network of contacts in nearly every geographic region of the world; and
- hosting the World Congress on IT, the only industry sponsored global IT event.

Founded in 1978 and originally known as the World Computing Services Industry Association, WITSA has increasingly assumed an active advocacy role in international public policy issues affecting the creation of a robust global information infrastructure, including:

- increasing competition through open markets and regulatory reform;
- protecting intellectual property;
- reducing tariff and non-tariff trade barriers to IT goods and services; and
- safeguarding the viability and continued growth of the Internet and electronic commerce.

Business Environment

In recent years, technology has drastically changed the way business is conducted. Today, information and capital flow freely and virtually instantaneously across borders in essentially every industry sector. The rate at which this change is taking place is a function of the rapid pace of change in technology.

The drivers of this change are digitization, convergence of computing and telecommunications, and the evolution of networking. Globalization and the decentralization of functions create the need for vast amounts of information to be transmitted across networks to business entities throughout the world.

For example, airlines transmit passenger reservation information from locations around the globe to a central facility where it is analyzed for load and revenue predictions which, are relayed to other analysts making decisions regarding the purchase of additional aircraft.

Manufacturers transmit sensitive engineering drawings and specifications from design centers to manufacturing locations. At the same time, production statistics and quality control data are flowing back to headquarters where the information is analyzed for release to world financial markets.

Pharmaceutical companies send details of new manufacturing processes to their plant locations for implementation. These new processes will create more effective drugs and at the same time improve the competitiveness of the parent company.

In short, sensitive business data is constantly traversing global networks, creating a robust and competitive business environment.

Emergence of a Problem

With sensitive information being sent throughout the world, business is naturally interested in insuring that it reaches and is used by only its intended recipients. In the past, the amount of data being transmitted was relatively small, and for the most part was sent over corporate private networks that provided a degree of security.

Business was relatively comfortable with law enforcement access to what was generally understood to be voice telephony. However, the world has changed. Open networks are more prevalent, data and voice are now both carried simultaneously in digital format, and information at the very heart of a corporation may now travel virtually anywhere en route to its destination. Suddenly, business has found itself in a new environment and the old rules no longer seem so acceptable.

On the one hand, business has prospered by aggressively changing its business practices to more fully utilize the capabilities of networks and information technology. This has had a very positive impact on the

growth and vitality of the information services market. Now, however, security concerns are threatening the continued growth of the use of networks to transmit sensitive business information that, in turn, is threatening the robustness of the information services industry. These security concerns need to be addressed.

Business Concerns

User Choice Of Encryption Is Limited

One of the best ways that business feels it can secure its information and ensure that it is easily available only to the intended recipients is to encrypt it. However, users are not able to use the encryption technology and strength they feel is required in all parts of the world. Some countries restrict its use while others prevent either its import or export. The result is that business is unable to freely choose the strength of encryption that it feels will adequately protect transmitted information uniformly in all countries.

Standards For Legal Access Are Not Consistent

Understandably, judicial and legal systems vary widely around the world. Business respects this diversity and has adapted to varying standards in each country. As technology and competition drive business to deliver even more sensitive information electronically, the chance of its capture during transmission increases, particularly in countries where the standards for its legal access are relatively low. Thus, the inability to properly secure that information using strong encryption, or the availability of easy accessible and often surreptitious key recovery schemes, are of particular concern.

The Potential for Misuse of Proprietary or Confidential Information

In some countries, strong ties between a business and a government may lead to the possibility of industrial espionage. This situation is exacerbated when information cannot be properly protected through encryption, when encryption keys may be easily obtained without knowledge or consent, or when legal safeguards are inadequate.

Legal Jurisdictions for Access Are Not Well Defined

Networking poses new and vexing questions for business regarding legal access. During a given interactive session, sensitive business information may be updated, added to and altered from several locations globally, virtually simultaneously. Questions remain as to whether the entire session is subject to legal access jurisdiction of only one of the countries involved. Similarly, some authorities are suggesting access to information available in any computer or device that is networked into their country.

WITSA Principles

Clearly, legal access to information in the networked environment of today poses many concerns and challenges to business. WITSA supports the following principles, which are consistent with those being developed by a number of other international business organizations:

1. Users should be free to choose the type and strength of encryption they feel is necessary to protect their information.
2. Legal access by any given jurisdiction shall only be to information actually stored in that jurisdiction at the time of proper judicial notification.
3. A business shall have no obligation to maintain the means to provide clear text of transmitted information, including e-mail, unless the information is stored on the business's facilities in a non-transitory manner at the time the information is properly requested and during the period of the proper legal request, and is accessible in clear text by the business.
4. Legal access requests should be specific, and limited in scope and duration.

5. There should be no requirement that encryption keys be filed or registered with any third party, either public or private.
6. In order to protect personal privacy, all personal information that is accessed for any reason must be protected by the accessing agency.
7. All information that has been accessed must be returned once legal proceedings are complete, and any copies of such information should be destroyed.

The World Information Technology and Services Alliance (WITSA)

WITSA consists of the national information industry representative bodies from around the world. Its role is to develop public policy positions on issues of concern to the information industry and present these positions to governments and international organizations. WITSA members are:

Argentina	Cámara de Empresas de Software y Servicios Informáticos (CESSI)
Australia	Australian Information Industry Association (AIIA)
Bangladesh	Bangladesh Computer Samity
Brazil	Sociedade de Usuários de Informática e Telecomunicações - Sao Paulo (Sucesu-SP)
Canada	Information Technology Association of Canada (ITAC)
China, Taipei	Information Service Industry Association of China, Taipei (CISA)
Colombia	Colombian Software Federation (Federación Colombiana de Software - FEDECOLSOFT)
Czech Republic	Association for Consulting to Business (Asociace Pro Poradenství v Podnikání - APP)
Finland	Information Technology Services Association (Tietotekniikan Palveluliitto - TIPAL)
France	Syntec Informatique
Germany	Bundesverband Informationstechnologien (BVITeV)
Greece	Federation of Hellenic Information Technology Enterprises (SEPE)
India	National Association of Software and Service Companies (NASSCOM)
Israel	Israeli Association of Software Houses (IASH)
Italy	Associazione Nazionale Aziende Servizi Informatica e Telematica
Japan	Japan Information Service Industry Association (JISA)
Malaysia	Association of the Computer Industry (PIKOM)
Mexico	Asociación Mexicana de la Industria de Tecnologías de Información (AMITI)
Mongolia	Mongolian National Information Technology Association
Morocco	L'Association des Professionnels de L'Informatique de la Bureautique et de la Telematique (APEBI)
Netherlands	Federation of Dutch Branch Associations in Information Technology (Federatie Nederlandse IT - FENIT)
New Zealand	Information Technology Association of New Zealand (ITANZ)
Poland	The Polish Chamber of Information Technology and Telecommunications (Polska Izba Informatyki i Telekomunikacji - PliiT)
Republic of Korea	Federation of Korean Information Industries (FKII)
Romania	IT&C Association of Romania (ATIC)
Singapore	Singapore Federation of the Computer Industry (SFCI)
Spain	Asociación Española de Empresas de Tecnologías de la Información (SEDISI)
Sweden	Swedish IT-companies' Organisation AB (Svenska IT-Företagens Organisation AB)
Thailand	The Association of Thai Computer Industry (ATCI)
United Kingdom	Computing Services & Software Association (CSSA)
United States	Information Technology Association of America (ITAA)
Zimbabwe	Computer Suppliers' Association of Zimbabwe (COMSA)