Chapter XLIX
Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism: The European Response

Ioannis P. Chochliouros
Hellenic Telecommunications Organization S.A. and University of Peloponnese, Greece

Anastasia S. Spiliopoulou
Hellenic Telecommunications Organization S.A., Greece

Stergios P. Chochliouros
Independent Consultant, Greece

ABSTRACT

Europe has entered a new phase of growth in its history, and characterized by the fast deployment of modern electronic communications networks and information systems in the broader scope of a competitive, dynamic and knowledge-based economy. Network and information security is an essential evolving concept among current strategic issues. These can impact on a wide range of existing/emerging policies, citizens' concerns, including the protection against crime and terrorist threats, and the adaptation of governance structures to effectively deal with such matters and to preserve national security, public safety and the economic well-being of the State. In this context, several measures (legal, regulatory and technical provisions) have been adopted by the European Union to ensure data protection, citizen privacy and the legitimate interest of legal persons. However, member states preserve the right to carry-out lawful interception of electronic communications, or take other measures such as retention of traffic data, when necessary, for exact and specific purposes, to preserve security and to meet the generally recognised objectives of preventing and combating crime and terrorism. The current work examines the "balance" between these two fundamental policy requirements, with the aim of offering a high level of protection in an area of liberty, security and justice.

INTRODUCTION

Electronic communication networks and information systems are now an essential part of the daily lives of European citizens and are fundamental "tools" to the success of the broader European economy (Chochliouros & Spiliopoulou-Chochliourou, 2005). Networks and information systems are converging and becoming increasingly interconnected, thus creating a variety of potential opportunities for all categories of "players" involved. An overwhelming number of employees use a mobile phone, a laptop, or a similar device to send or retrieve information for work. Such information can represent a considerable value, for instance, describing a business transaction or containing technical knowledge. Moreover, Europe's rapid transition towards an innovative information society is being marked by profound developments in all aspects of human life: work, education, leisure, government, industry, and trade. The new information and communication technologies are having a revolutionary and fundamental impact on our economies and societies. In fact, the success of the information society is important for growth, competitiveness, and employment opportunities and has far-reaching economic, social, and legal implications. However, in the hands of persons acting in bad faith, malice, or grave negligence, information society technologies (ISTs) may become tools for activities that endanger or injure, the life, property, or dignity of individuals or even damage the public interest (European Commission, 2001c).

Despite the many and obvious benefits of the modern electronic communications development, it has also brought with it the worrying threat of intentional attacks against information systems and network platforms/infrastructures. As cyberspace gets more and more complex and its components more and more sophisticated, especially due to the fast development and evolution of (broadband) Internet-based platforms, new and unforeseen vulnerabilities may emerge (European Commission, 2001b). These attacks can take a wide variety of forms including illegal access, spread of malicious code, and denial of service attacks. Unfortunately, it is possible to launch an attack from anywhere in the world, to anywhere in the world, at any time (Eloff & von Solms, 2000).

Some of the most serious incidents of attacks against information systems are directed against electronic communications network operators and service providers or against electronic commerce companies. More traditional areas also can be severely affected (PriceWaterhouseCoopers, 2001), given the everincreasing amount of interconnectivity in the modern communications environment: manufacturing industries, service industries, hospitals, other public sector organizations, and governments themselves. But victims of attacks are not only organizations; there can be very direct, serious and damaging effects on individuals as well. The economic burden imposed by these attacks on public bodies, companies, and individuals is considerable and threatens to make information systems more costly and less affordable to users. Consequently, as so much depends on networks and information systems, their secure functioning has become a key concern.

BACKGROUND: CURRENT EUROPEAN RESPONSES FOR INCREASED SECURITY

In order to fully support the importance of the transition to a competitive, dynamic, and knowledge-based economy, the European Commission launched the *e*Europe initiative, (accompanied by a proper Action Plan) to ensure that Europeans can reap the benefits of the digital technologies and that the emerging information society is socially inclusive (European Commission, 2002). In particular, the Action Plan highlights the importance of network security and the fight against cybercrime (European Commission, 2001a).

Information and communication infrastructures have become a critical part of the backbone of modern economies. Users should be able to rely on the availability of information services and have the confidence that their communications and data are safe from unauthorized access or modification. However,