Enterprise Security: Legal Challenges and Possible Solutions

Emily M. Weitzenboeck
Norwegian Research Centre for Computers & Law, University of Oslo
emily.weitzenboeck@jus.uio.no

Abstract

To survive in the business, especially the online world, an enterprise requires an effective security infrastructure. However, enterprises should bear in mind that there is often also a legal obligation to keep certain data or information secure, emanating from legislation such as intellectual property, data protection or trade secret legislation or from contract. A number of technological measures already exist to provide security in the online world, such as encryption, electronic signatures and privacy enhancing technologies. However, one often encounters a number of legal constraints to the use of these measures through, for example, restrictions on the export and use of cryptography, difficulties and doubts of the legal recognition of electronic signatures, and different national rules on certification services. If electronic commerce is to grow, there is need for more international co-operation as well as mutual recognition of, and more liberalisation of, such regulations.

1. Introduction

Any business needs to maintain a degree of security over its information, be it personal data, intellectual property protected information or other confidential information. Where such a business uses electronic means of data storage and has connections to the outside world via the Internet, there is the additional risk of external attack. The loss, destruction, disclosure or improper use of data and/or information can lead to a liability claim against the business. Hence the need for a proper and effective security infrastructure.

2. Legal obligation of security

It is not merely good business sense to keep information such as commercially sensitive information and client or employee personal data, confidential. There is also, very often, a legal obligation to keep such data or information secure or confidential. This duty may be (i) statutory or (ii) contractual.

2.1. Statutory obligations

A statutory obligation to keep data or information secure may, in turn, arise from obligations imposed by intellectual property legislation, data protection or privacy legislation, and trade secret laws. Thus, for example, the inventor or proprietor of an invention should keep the invention secret at least until the date of filing of a European patent application, as otherwise the invention would not be considered to be novel and patentable (Article 54, European Patent Convention). The European Union’s (“EU”) Data Protection Directive [1] imposes a duty of security on the controller of personal data, i.e. on data relating to an identified or identifiable natural person. The data controller should “implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.” (Article 17). Member States of the EU had to implement the EU Data Protection Directive by October 1998. European businesses that do not have proper security measures will be deemed to be in breach of the national data protection law which implements this Directive.

A similar obligation of security is found in the Safe Harbor Privacy Principles [2] recently agreed to by the
EU and the U.S., viz. that “organisations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorised access, disclosure, alteration and destruction.”

Although the Safe Harbor Privacy Principles are entirely voluntary for U.S. businesses, if such a business wants to engage in trade with an enterprise in an EU country and this entails the transfer of personal data from the EU country, then this U.S. business would have to comply with the Safe Harbor Privacy Principles. This is because transfer of personal data to countries outside the EU is prohibited by the Directive unless such country ensures an adequate level of protection. The Safe Harbor Privacy Principles are meant to provide such adequate level of protection.

The question that naturally arises is whether other countries outside the EU have adequate level of protection and how is this to be determined by the enterprise wishing to transfer such data. The EU Directive does provide a number of criteria such as the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law in force in the country in question, and the professional rules and security measures which are complied with in that country. However, it is not easy for an enterprise to determine whether and when a third country fulfils these criteria. One way forward would be to increase the use of “safe harbor-like” agreements in other countries, coupled with a good dissemination strategy on the advantages of the use of such schemes.

Besides intellectual property and data protection or privacy-related legislation, a business may be bound to keep certain information secret under trade secret law. A trade secret is commercially valuable information which is not in the public domain and is the subject of reasonable efforts to maintain its secrecy. For example, the North American Free Trade Agreement (NAFTA) obliged member countries to protect trade secrets from unauthorised acquisition, disclosure or use. Similarly, the Trade-Related Aspects of Intellectual Property Rights or TRIPs Agreement provides protection for “undisclosed information”.

2.2. Contractual obligations

An obligation to keep secure information systems may also stem from the contractual undertakings of an enterprise. For example, a contract may contain a confidentiality clause by means of which the enterprise has undertaken a contractual obligation to keep certain information confidential. Breach of such a clause would lead to the enterprise being in breach of contract and becoming liable for payment of damages.

A business should also maintain security of its information systems to ensure and safeguard data integrity (in the sense that a message that has been transmitted over the Internet was properly received) and authenticity (in the sense that the message which the recipient receives is identical to that transmitted by the sender).

3. Mechanisms to ensure security

Both legal, and technical and organisational measures may be taken to ensure that an information system is secure.

3.1. Legal mechanisms

As already mentioned above, an obligation of confidentiality and a duty of non-disclosure may be inserted as a contractual condition. A contract may stipulate that breach of such a clause will make the party in default liable for the payment of damages. In countries with a civil law system [3], one may come across a pre-liquidated damages clause which provides that a specified sum of money becomes payable as damages to the injured party upon such disclosure or breach of confidentiality.

Caution should, however, be taken with the use of such clauses since, if the amount is too low, it will only serve as a means for the other party to get out of its contractual obligations by opting to pay the damages; if it is disproportionately high, it might be deemed to be excessive and a penalty clause, and is therefore likely to be reduced by a trial judge.

Moreover, common law systems (such as the UK, US), although allowing the use of preliquidated damages clauses, are reluctant to enforce contractual penalty clauses on grounds of public policy. The UK Court of Appeal holds that, although an innocent party can sue on the penal clause, “it will not be enforced … beyond the sum which represents [his] actual loss” [4].

3.2. Technical and organisational measures

Many enterprises spend large sums of money to protect their networks and intellectual property against
intrusion from the outside world by installing firewalls and protective software. However, if such enterprises still continue to e-mail confidential and private information without any technological protection, there is the risk that such information is intercepted. This exposes them to fraud, industrial espionage, and damaging risks and liabilities. Encryption, electronic signatures, and privacy enhancing technologies (sometimes abbreviated as PETs) are measures to safeguard confidential traffic over the Internet.

In private key encryption, where each party has the same private key, the message is encrypted by the sender with the key and subsequently decrypted by the recipient with the same key. In public key encryption, the message is encrypted with the recipient’s public key and the recipient can decrypt it with his own private key. In public key encryption, each party has two keys: a public key which is published to the public at large, and a private key which must be kept secret.

Cryptography may also be used to ensure message authenticity and data integrity, through the use of electronic signature technology using public key cryptography. This is done by the sender encrypting a document with his/her private key. Any third party may decrypt the message using the sender’s public key which corresponds only to the sender’s private key. If the document is successfully decrypted, then one has the necessary assurance that it could only have been created by that sender, as otherwise one would not have been able to decode it.

The use of technological measures to prevent unauthorised access to personal data is also an important part of a business’ efforts to ensure privacy. However, this does not equal privacy protection, the latter being a wider concept which starts with the initial collection of the data by ensuring that there is a good reason to do so, and that its use will be restricted to legitimate ones of which the data subject would have been advised. Once the data has been collected, security and confidentiality become paramount. Therefore it is important that businesses which control databases of identifiable personal data, should have a proper organisational and policy setup with regards to the collection, use, storage, disclosure and destruction of such data. This is also a legal requirement in Europe as a result of legislation such as the Data Protection Directive, the Council of Europe Convention 108 [5], the various national data protection laws, not to mention the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (September 1980) to which other non-European countries also adhere.

One way of ensuring privacy protection of personal data is to control the instances where the individual’s true identity is released within the information system through the use of what is known as an identity protector. Put simply, its effect is to cordon off certain areas of the system which do not require access to true identity. One of the most important functions of the identity protector is to convert a user’s actual identity into a pseudo-identity, an alternate (digital) identity that the user may adopt when using the system. As explained in a report by the Dutch Registratiekamer [6] on privacy enhancing technologies:

“...When an identity protector is introduced into an information system, two domains are created: an identity domain and a pseudo domain, one in which the user’s identity is known and accessible, and one in which it is not. The identity protector separates the two domains and may be applied anywhere in the system where personal data can be accessed. A simple guideline for designers of new information systems is to minimise the identity domain wherever possible and maximise the pseudo domain.”

Encryption techniques involving digital signatures, blind signatures, digital pseudonyms and trusted third parties may be used as PETs.

4. Legal difficulties arising from the use of cryptography

Cryptography may therefore address both issues of confidentiality (through the use of encryption technology) as well as message authenticity and data integrity (through the use of digital signatures using public key cryptography).

However, the problem that arises is whether the use of encryption technology is permitted and legal. Historically, governments have considered encryption technologies as "dual use goods" in that they may be used both for a civil as well as a military purpose. However, national laws vary in their treatment of cryptographic equipment and software and the domestic sale, possession, use and importation thereof as well as the export of such products may be subject to controls and restrictions under national law, regional law (such as EU law), and in terms of the state’s international obligations.

These various controls constitute a significant regulatory burden on businesses in countries where
there are such controls, and delay the transfer of strong cryptography, the protection of personal data, and the growth of Internet commerce [7].

4.1. The Wassenaar Arrangement

In the Wassenaar Arrangement, cryptography is controlled as "information security” and is designated as a sensitive dual-use item under Category 5 Part 2 of the dual-use list.

In December 1998, the Wassenaar member states agreed on new export control rules for encryption techniques. Export controls were relaxed and it was provided that in future products with a symmetric algorithm will only be subject to export controls if they have a key length of at least 56 bits.

Broadly speaking, the trend internationally has been towards a gradual move for further relaxation of controls and, in fact, as of December 2000, the Wassenaar Arrangement provides that mass market software and hardware which satisfies certain conditions laid down in the Cryptography Note is not subject to export controls [8].

The Wassenaar Arrangement is not an international treaty but is merely designed to allow the Participating States to exchange views and information on international trade in conventional arms and dual-use goods and technologies. Participating States commit to adjust their national export control policies to adhere to the Wassenaar Arrangement Control Lists, but this commitment is discretionary in nature and not mandatory. In fact, a number of states have more stringent controls on encryption than those laid down in the Wassenaar Arrangement (e.g. Russia). However, the EU has generally followed the list of controlled goods of the Wassenaar Arrangement.

4.2. The EU Regulation

Fairly recent developments in the EU will facilitate the movement of dual-use goods, including cryptography, among EU states and between EU states and the following ten countries: Australia, Canada, the Czech Republic, Hungary, Japan, New Zealand, Norway, Poland, Switzerland and the U.S. A new Council Regulation No. 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology was published on the 30th June 2000 (the “Dual-Use Regulation”). It entered into force on the 29th September 2000 and replaces the earlier 1994 Council Regulation No. 3381/94. As an EU Regulation, it is directly applicable in the territory of all the EU Member States, and constitutes direct legislation by the Community.

According to this new Regulation, the transfer or movement of dual-use goods from one EU member state to another is entirely liberalised, with the exception of some highly specialised cryptanalysis products. An individual export authorisation is required for certain specialised products (Annex IV of the Regulation).

The EU Regulation creates a harmonised licence system – the Community General Export Authorisation – for export of dual-use goods and technology (except for cryptanalysis products) from the EU to any one of its abovementioned ten trading partners.

4.3. Some national laws

The Dual-Use Regulation is likely to trigger off similar relaxation of controls of dual-use goods in the other ten non-EU member states to which favourable treatment has been given.

In fact, the U.S. has already implemented a liberalisation of export controls on encryption products from 19 October 2000. Under the new U.S. policy announced on 17th July 2000, U.S. companies can export, without need of a license, any encryption product to any end user in the 15 nations of the EU as well as Australia, Norway, Czech Republic, Hungary, Poland, Japan, New Zealand and Switzerland. US exports are permitted to ship their products to these nations immediately after they have submitted a commodity classification request for their product to the Department of Commerce. Exports thus no longer have to wait for a completed technical review or incur a 30-day delay to ship their encryption products to customers in these countries.

4.4. Other domestic controls

The other type of control on encryption is domestic control and may involve the requirement for encryption keys and sensitive information to be handed over to third parties (which in many cases are government agencies). Such controls are controversial and have been seen to impinge on basic rights such as the right to personal privacy, freedom of speech and the right of association, as well as raising questions about the
power of governments to carry out ‘ad hoc’ searches [9].

Most EU Member States have no restrictions on the use or importation of cryptography. Some have minor controls such as ordering that encrypted data be converted into an intelligible form following a police search and seizure (e.g. Ireland) while other countries (e.g. U.K.) have gone a step further and require that, in such search and seizure situations, the decryption key itself should be provided.

France has restricted the domestic use and supply of cryptography for a long time but, following a speech by Prime Minister Jospin in January 1999, it appears that the domestic use and the import of cryptography will be liberalised in the long term.

Controls on the export, use and/or importation of cryptography as well as the different national legal provisions on this matter hamper the use of strong cryptography. Recent efforts by the European Union and the U.S. to ease such controls are a large step towards relaxing such restrictions and it is hoped that this trend is not reversed.

5. Legal obstacles to the use of electronic signatures

Although electronic signatures provide the same, if not better, authentication of a document as a written signature, one may encounter legal constraints and difficulties as to the use and/or validity of electronic signatures. Difficulties arise, where a particular statute requires that a document be in writing or that it should be signed, as to whether an electronic document which is digitally signed would be considered to be in fact a “writing” and “signed”. The problem is compounded by the fact that the status and legal recognition of electronic signatures and electronic documents may vary from one country to another, a fact which may hamper electronic commerce which, of its very nature, is not bound by traditional geographical boundaries.

This situation has been recognised both at an international and national level, with bodies like the United Nations Commission on International Trade Law (UNCITRAL) and the European Union promoting a change or adaptation of traditional paper-based laws. In fact the UNCITRAL Model Law on Electronic Commerce of 1996 contains a model clause which provides equivalent recognition of electronic signatures (Article 7), a model on which Article 10 of the Electronic Transactions Act 1999 of Australia [10] is based.

In the U.S., an electronic signature cannot be denied legal effect solely because it is in electronic form as opposed to paper (subject to listed exceptions). This has been stated in the Electronic Signatures in Global and National Commerce Act 2000 Section (101(a)(1)), the Uniform Electronic Transactions Act 1999 (Section 7), while the Uniform Computer Information Transactions Act 1999 has a similar provision with regards to electronic authentication (Section 107).

The need for legal recognition of electronic signatures and for a harmonised legal framework was also recognised in the EU Electronic Signatures Directive[11] which should be implemented by the EU member states before 19 July 2001. According to the Directive, EU states are to ensure that advanced electronic signatures which are created by a secure-signature-creation device, (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data, and (b) are admissible as evidence in legal proceedings. It also provides that an electronic signature should not be denied legal effectiveness or admissibility solely on the ground that it is in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure signature-creation device.

Problems still may arise where, and if, legal recognition is not carried out in a harmonised way, since such different legal requirements in national laws may constitute a barrier to international trade. The same applies to the legal recognition of certification services, which is also regulated in the EU by the Electronic Signatures Directive.

Qualified certificates issued in a country outside the EU are recognised as legally equivalent to certificates issued within the Community where (a) the Certification Service Provider fulfils the requirements of the Directive and has been accredited under a voluntary accreditation scheme established in a Member State, or (b) a Certification Service Provider established within the Community which fulfils the requirements laid down in the Directive guarantees the certificate, or (c) the certificate or the Certification Service Provider is recognised under a bilateral or
multilateral agreement between the Community and third countries or international organisations.

The need for the development of cross-order arrangements was recognised by the EU in the Electronic Signatures Directive in preamble 23 that “in order to ensure interoperability at a global level, agreements on multilateral rules with third countries on mutual recognition of certification services could be beneficial.”

6. Conclusions

An efficient and secure information and communications technology infrastructure enables a company to participate in new forms of business co-operation such as virtual enterprises, of which secure co-operation is an important aspect.

While a number of technological measures already exist and more advanced measures are under development, a number of legal constraints to the effective use of such measures also exist. The EU Dual-Use Regulation and the corresponding US liberalisation initiative in 2000 are a step in the right direction, but far from a satisfactory solution as they apply to a determinate list of countries. The difficulty is due to the fact that encryption technology is often viewed as a powerful weapon in the wrong hands, be they the hands of the enemy-at-war or a criminal organisation. However, the answer, it is felt, is not to prohibit or excessively restrict the use of such technologies, since such restrictions would only fetter law-abiding citizens and not enemies or criminals who would still manage to obtain such technology underground. There are other channels through which states could fight organised crimes more effectively.

Countries that do not want to be left out of the e-commerce boom should adapt their laws to give legal effect and validity to electronic contracts and electronic signatures, such as the European Union and the United States have done. Efforts should also be concentrated at ironing out conflicts of laws among different jurisdictions through co-operation, mutual recognition and harmonisation at an international level such as through international initiatives like the ongoing negotiations at the Hague Conference on Jurisdiction.

7. Acknowledgement

Part of this article is based on research carried out by the author during participation in the research project MARVIN (MARitime Virtual enterprise Network – EP 29049) which is funded by the European Commission and is part of the ESPRIT project framework. The views expressed in this paper represent the author’s exclusive views and have not been endorsed by the Commission.

8. References