Appendix 1
Legal Memorandum

TASCA Law Firm

Legal memo – Important notice (1/2)

- We have been asked to write a legal memo to examine and evaluate the possibility to use systems of computerized cryptography, particularly those activated through a crypto-dynamic method, in "non-voice" telecommunications – i.e., the transmission of SMS (Short Message Service) and MMS (Multimedia Messaging Service) files, as well as electronic data transmission such as e-mail communication, and transfer through the World Wide Web of electronic files of any format.
- We have been asked also to extend our analysis of the legislative, policy and legal aspects of the matter at hand pertaining to the use crypto-dynamic methods in the digital publishing sector, and particularly in the transfer and sale of digital format texts to e-book users.
- Such analysis shall take into consideration the following facts:
  - our client intends to create a start-up business in the Information Technology sector, with the purpose of commercializing IT and telecommunication services, consisting in generating and selling <<crypto-dynamic keys>>, functional to the ciphering of SMS-MMS, e-mail, and electronic files of any format, including e-book texts.
  - our client has elaborated its own <<technology>> based on an algorithm, consisting in an *original* and *innovative* system of generation and decryption of the cryptographic keys, for which invention it has filed an international PCT patent application, which is currently pending.

Legal memo – Important notice (2/2)

➢ This legal memorandum focuses on the questions:

a. Whether national and international policies, including also guidelines and regulations, particularly those issued by the EU, are compatible with the use of cryptographic techniques, particularly with "crypto-dynamic" techniques in <<**non-voice telecommunication**>> via SMS-MMS text transfer;

b. Whether national and international policies, as outlined above, are compatible with the use of "crypto-dynamic" techniques in <<**data-transfer communication**>> of electronic files via e-mail and messaging services on social network platforms;

c. Whether national and international policies, as outlined above, are compatible with the **electronic transfer of published or unpublished texts** protected under intellectual property laws (rights of authorship).

Legal memo – The crypto-dynamic system

- The system invented and arranged by our client is a *centralized cryptographic system*. Such system is capable of adding to the ciphering of data a number of parameters that may be utilized to set readability conditions and manage at will the use of such data, whether they are transferred through non-voice telecommunication systems or through electronic communication via the Web.
- Such ciphering is of the symmetric type, and the company specifies and highlights, in its request for a legal memorandum, that **the key generated does not exceed 56 bits** (the relevance of such feature shall be object of further explanation).
- The term "dynamic", in its most traditional and common connotation indicates and implies that a key is generated in accordance with a specific event, a characteristic that does not apply to digital signature technology, where two keys – of the asymmetric type - are fixed and unchanging, and are associated to a specific physical person.
- In the case at hand the ciphered information is subjected to additional parameters, which cause such key to behave differently at various points in time, in a <<dynamic>> fashion. For such original and innovative feature the system uses a new ciphering algorithm, subject to acquiring patent rights, and an underlying and customized *database*.
- The system is centralized in the sense that potential users access such system to cipher their electronic files (obtaining a key through an exchange of information managed under SSL – *Secure Sockets Layer* – safety protocol), and establish a set of additional parameters according to need.
- It is, therefore, an original and innovative creative approach distinguished by unique features, not to be confused with PEC or digital signature systems, which are characterized by wholly different techniques, and are typically regulated by a different discipline, which, at the European as well as the local level, is generally thorough and specific; nonetheless, the International Community has adopted a different approach with regards to norms, regulations and control issues.

TASCA Law Firm
Legal Advisor

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (1/13)

- The first political document on this matter, at the international level, was the ***Wassenaar Arrangement***, first multilateral agreement, on a global scale, to intervene on the criteria and approach of the international community towards technologies susceptible of being of <<double use>>, civil and military, seen under one single evaluation perspective, with the export of conventional weapons and materials of double use.
- Such document was not directed against any particular State, as it merely implemented one of the funding principles of the United Nations: work towards international cooperation and technologic development, with the shared commitment of countering international terrorism, taking a firm stand against those Nations that adopt an hostile approach towards the international community.
- The primary purpose of the agreement was, thus, to synchronize the need for joint actions – adopted politically first, and translated into legislation later – trying to contrast transfers of weapons or technologies that may strengthen operations, organizations or Nations effectively active in their support of terrorism, compromising international peace and stability.
- Its final version was drafted by thirty-one countries, including Argentina, Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Holland, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Commonwealth of Independent States, Slovak Republic, Spain, Sweden, Switzerland, Turkey, United Kingdom, and United States of America. Later Bulgaria and Ucraine adopted the agreement.

TASCA Law Firm
Legal Advisor

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (2/13)

- Cryptography, in the Wassenaar Arrangement, generally, but with certain very specific, significant, nullifying exceptions, is regarded and classified as *dual-use good*, due to the ambivalence of its utilization as a means to secure privacy and as a potential offensive tool, and, as such, of possible utilization in warfare.
- Therefore both cryptography in and of itself, as well as the technology pre-ordained to be utilized in conjunction with it, are included in the <<list>> of double-use goods and technologies – specifically as part of Category 5, part 2, "***Information security***".
- Such category includes both hardware and software products.
- Escaping the control on exportation, and constituting the exceptions conceded by the Wassenaar Arrangement, are certain types of technology or goods: such are the **products listed in point 5.A.2**, among which, as further detailed below, may – unless expressly prohibited by the States – include the electronic products connected with "Cryptodynamics".
- The political and conceptual grounds - not at all devoid of technical considerations - on which the international community of Wassenaar laid its position, was such as to allow the obtainment, in the main, of the liberalization of exportation and trade of ***mass software*** or software of public domain; such policy came from the general provision contained in the agreement, which is widely known as ***General Software Note***.
- Particularly, the provision allows the free exportation of all the cryptographic products with a symmetric key not exceeding 56 bit, or an asymmetric key not exceeding 512 bit; it also allows the free exportation of all the products based on cryptography (independent of any key) not exceeding 112 bit.

TASCA Law Firm
Legal Advisor

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (3/13)

- Particularly, the Arrangement adopts an exclusion system: it allows the free exportation of *mass cryptographic software and hardware* based on keys (with the limitations above indicated), as well as the free exportation of products that use cryptographic systems for the protection of intellectual property, while the exportation of anything not specified in the list under point 5.A.2 is still subject to the obtainment of authorization.
- Not every member State of the Wassenaar Arrangement, however, accepted the dispositions contained in the General Software Note, and in particular Australia, France and New Zealand continue to control the exportation of cryptographic software, irrespective of its being "mass" or "of public dominion".
- Nonetheless, the provisions of the Wassenaar Arrangement, which was a mere political agreement and not a Treaty, need to be adopted in the respective legal system of the single adhering States, through their own statutory provisions. Each State's internal laws might, in turn, either restrict or broaden the terms of this type of international agreements.
- The States that participated and were involved in the panel have adopted different regulations on their national level, and the same difference was registered in EU regulations and directives.
- Particularly relevant is EU Regulation No. 1334/2000, later amended with EU Regulation No. 1167/2008. States like Italy, for example, have aligned such regulations with their internal law, in the case of Italy with Legislative Decree No. 96/2003 and Decree of August 4, 2003 (published in the Official Gazette of September 1, 2003, No. 202), as similar legislative actions were taken by nations like France, the United Kingdom, and Germany.

TASCA Law Firm
Legal Advisor

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (4/13)

- Yet today the internal legislations of EU States seem to be left behind by the newest EU Regulation No. 428/2009 of May 5, 2009, which has instituted a clear EU regime of control on the exportation, transfer, intermediation, and transit of double-use products.
- As of today, thus, the dispositions of EU Regulation 428/2009 are immediately applicable in member countries of the European Union, including Italy.
- As we well know, the essential characteristic of EU Regulations is their immediate applicability in national territories, which can't be said about Directives, which do not require any act of receipt or transposition.
- Immediate applicability, however, does not exclude that the States may intervene with supplementary or implementation provisions of such Regulation (which may occur when, for instance, member States are required to fix the amount of penalties or other fees). They are remain mandatory and binding in all their parts (*general application*), meaning that member States are bound to apply them in their entirety, with no repeals or modifications of any kind.
- The courts of each member State are required to directly apply community regulations, overruling conflicting internal laws. Having taking into consideration such context of legislative hierarchy, let us consider how cryptography technology, involving the ciphering of documents and their cancellation or programmed readability, may definitely, **abstractly**, be classified as a *double use* technology, having dual civil and military use pursuant to EU Regulation No. 428/2009. Thus, the utilization or the exportation/importation of products connected with "cripto-dynamics" may be subject to EU Regulation No. 428/2009 in EU member States. In relation to such extend and specific interpretation we need to examine two distinct hypotheses, in order to outline the laws **concretely** applicable.

TASCA Law Firm
Legal Advisor

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (5/13)

Hypothesis No. 1 (1/5)

- The Regulation deals with goods – systems, equipment, and components – utilizing cryptography within the scope of Annex 1 – Category 5 "Telecommunications and information security" – Part 2 "Information Security" – page. 167.
- Note 3, on page 167, specifically states:

Cryptography Note

- 5A002 and 5D002 **do not control** goods that meet all of the following:
  a. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
     1. Over-the-counter transactions;
     2. Mail order transactions;
     3. **Electronic transactions**; or
     4. **Telephone call transactions**;
  b. The cryptographic functionality **cannot easily be changed by the user**;
  c. Designed for installation by the user **without further substantial support by the supplier**; and
  d. When necessary, **details of the goods are accessible and will be provided, upon request, to the competent authorities of the Member State in which the exporter is established** in order to ascertain compliance with conditions described in paragraphs a. to c. above.

TASCA Law Firm
Legal Advisor

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (6/13)

Hypothesis No. 1 (2/5)

Let us proceed with the analysis of the case at hand and of the SMS-MMS crypto-dynamic product.

- Such product is a message not exceeding 140 characters, transmitted through "non-voice" communication – thus not subject to the restrictions and inhibitions imposed on "voice" cryptography – substantially a synthetic form of "correspondence" among private individuals.
- In the case of the crypto-dynamic SMS product the communication takes form through the transmission of an actual "envelope" ( ) via telephone, containing a written message that only the crypto-dynamic key can decode and unveil to the receiver.
- **Such form of correspondence and data transfer may be classified as "electronic transaction", point a.3 of the cryptography note, or as "telephone call transaction", point a.4 of the cryptography note above.**
- Additionally, on the recurrence of the requirements of letter a), the goods are made "***available to the public by being sold, without restriction***" (note No. 3 – Annex 1 – Part 2 of EU Regulation No. 428/2009).
- A further interpretation and evaluation of the provision under letter **b)**, leads to the patent conclusion that the cryptographic function ***cannot be easily changed by the user***.
- Similarly, as per letter **c)**, the Smartphone applications are *designed for installation by the user, through download,* ***without further substantial support by the supplier***.
- Nonetheless there is no doubt that the requirement of letter **d)** - ***details of the goods are accessible and will be provided, upon request, to the competent authorities of the Member State in which the exporter is established*** - apply to the case at hand.

TASCA Law Firm
Legal Advisor

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (7/13)

Hypothesis No. 1 (3/5)

- Our client has in fact specified that the system is characterized by its capacity to record, memorize and retain all the keys generated, which are made available – at the same moment they are generated – to the phone service provider and thus to the "***competent authorities of the Member State in which the exporter is established***".
- From such analysis we may reasonably conclude that the crypto-dynamic technology is not subject to any authorization in the exportation of its products within the European Community, in view of the following facts:
  - **Both of the "excluding" criteria listed in letter a) apply to the transmission of the client's products**
  - **the requirement listed under letter b) applies**
  - **the requirement listed under letter c) applies**
  - **the condition noted in letter d) applies.**
- It thus appears evident that the products our client intends to commercialize fall squarely within Category 5 – Part 2 – Annex I to the Regulation – pages 167-174, Note 3.

TASCA Law Firm
Legal Advisor

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (8/13)

Hypothesis No. 1 (4/5)

- **Furthermore, according to Category 5 – Part 2 – Annex I to the Regulation – pages 167-174, Note 3, test-inspection-production equipment, and crypto-dynamic software and exportable technology are expressly not subject to authorization**. That can be clearly by the remaining dispositions of Category 5 – Part 2 – Annex I to the Regulations pages 167174:
  - *"5B2Test, Inspection and Production Equipment*
  - *5B002"Information security" test, inspection and "production" equipment, as follows:*
    a. *Equipment specially designed for the "development" or "production" of equipment specified in 5A002or 5B002.b.;*
    b. *Measuring equipment specially designed to evaluate and validate the "information security" functions ofthe equipment specified in 5A002 or "software" specified in 5D002.a. or 5D002.c.*

  […]
  - *5D002 **does not control** "software" as follows:*
    a. *"Software" required for the "use" of equipment excluded from control by the Note to 5A002;*
    b. *"Software" providing any of the functions of equipment excluded from control by the Note to 5A002.*
    c. *[…]*
  - *5E2Technology*
  - *5E002"Technology" according to the General Technology Note for the "development", "production" or "use" of equipment specified in 5A002, 5B002 or "software" specified in 5D002.a. or 5D002.c.*

TASCA Law Firm

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (9/13)

Hypothesis No. 1 (5/5)

- From the conclusions thus far illustrated it follows that if the "Cryptodynamics" telecommunication applications for the transfer of SMS – MMS correspondence – excluding any "voice" transmission – shall maintain all of their characteristics as above described, it appears to be unnecessary, to further analyse the issue relating to the length of the symmetric algorithm key used (> or < 56 bit) or the additional characteristics listed in Category 5 – Part 2 – Annex I to the Regulations, pages 167-174, for the purpose of researching possible grounds for exclusion from authorization.

* * *

Nonetheless, we deem it useful to formulate an alternative and secondary scenario, differing from the first hypothesis, should our conclusions be deemed unsuited, regarding our interpretation of the product's nature and transmission characteristics, which, in our opinion, place the product within the categories excluded from authorization, or in case our clients decide to modify the systems and characteristics of the product, failing to fall within the excluding classifications.

TASCA Law Firm

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (10/13)

Hypothesis No. 2 (1/4)

- The Regulation addresses cryptography goods (systems, equipment, and components) in Annex 1 – Category 5 "Telecommunication and Information Safety" – Part 2 "Information Safety" – pages 167-174.
- On page 167 we read that are subject to authorization the "*Systems, equipment, application specific "electronic assemblies", modules and integrated circuits for "information security", as follows and other specially designed components therefore*" when they are:

1. *Designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature and having any of the following:*
    1. *Authentication and digital signature functions include their associated key management function.*
    2. *Authentication includes all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, Personal Identification Numbers (PINs) or similar data to prevent unauthorised access.*
    3. *"Cryptography" does not include "fixed" data compression or coding techniques.*

***Note**: 5A002.a.1. includes equipment designed or modified to use "cryptography" employing analogue principles when implemented with digital techniques.*

a. A "symmetric algorithm" employing a key length in excess of 56 bits;

b. [...]

TASCA Law Firm
Legal Advisor

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (11/13)

Hypothesis No. 2 (2/4)

2. *Designed or modified to perform cryptanalytic functions;*
3. *Not used;*
4. *Specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;*
5. *Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, other than those specified in 5A002.a.6., including the hopping code for "frequency hopping" systems;*
6. *or network identification codes, for systems using ultra-wideband modulation techniques and having any of the following:*
   a. *A bandwidth exceeding 500 MHz; or*
   b. *A "fractional bandwidth" of 20 % or more;*
7. *Non-cryptographic information and communications technology (ICT) security systems and devices evaluated to an assurance level exceeding class EAL-6 (evaluation assurance level) of the Common Criteria (CC) or equivalent;*
8. *Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;*
9. *Designed or modified to use "quantum cryptography".*

TASCA Law Firm

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (12/13)

Hypothesis No. 2 (3/4)

- Applying the regulation to the case at hand, the "*Systems, equipment, application specific "electronic assemblies*" utilizing Cryptodynamics, particularly those finalized at SMS/MMS applications – but not only, as we add to our evaluation and analysis also those utilized in electronic communication [e-mail] – it is reasonable to presume that more than one of the conditions detailed in points 1.1, 1.2, and 1.3 may theoretically apply.
- However, note 5A002.a.1, with the specific function of clarifying and defining the boundaries of the limitations discussed, specifies, in point a) that the numeric techniques that carry out cryptographic functions are not excluded altogether by default (where, by exclusion, means requiring authorization); such exclusion is limited only to those functions based on analogical principles that use numeric techniques that produce a ***"symmetric algorithm" employing a key length in excess of 56 bits***".
- Thus, the use of a symmetric algorithm employing a key length exceeding 56 bits remains the determining criterion.
- Our client asserts that his technology, developed based on a patented process, including Cryptodynamic products, shall, n any case, utilize keys shorter than 56 bits – that applying to electronic communication and the transmission of the electronic files connected, attached, or associated thereto, and particularly for telecommunication through SMS/MMS.

TASCA Law Firm

Legal memo - Compatibility of Crytpodynamics with the regulations relating to the exportation of <<double use>> products and technologies in the European Community, and from the European Community to foreign countries (13/13)

Hypothesis No. 2 (4/4)

- Conclusively, we must address also to the fact that, where our client decided to utilize, for its products, technology generating symmetric keys exceeding 56 bits in length, his activity would not altogether be precluded or inhibited as being unlawful, illegitimate, or against laws and/or regulations. Our client may indeed continue to exercise his activity once he shall have requested and obtained the required authorizations.
- The condition to obtain such authorizations, we must observe, is not wholly excluded, even under the current key length, with regard to the exportation towards certain countries considered "at risk", and towards which the international community (particularly the European Union) exercises particular caution, such as Nigeria, North Korea, and Iran.
- As to the latter, for which was issued a specific restrictive regulation (EU Regulation No. 1128/2009; followed by Legislative Decree No. 64/2009 in Italy), the international community is moving towards a sort of embargo. The proposal is to make all the dual-use goods, as defined in Annex 1 to EU Regulation 428/2009, non-exportable and banned towards Iran. Supplementary controls are also disposed for all traffic towards "rogue states" of the Mediterranean, which, as revealed by suspect reported activities, may provide a doorway to the Countries mentioned above.
- Further information on guidelines and application forms for the obtainment of exporting authorization for double-use goods may be found on the website: http://www.mincomes.it/dualuse/dualuse.htm .

TASCA Law Firm
Legal Advisor

Legal memo - Compatibility of "Criptodynamics" with the norms regulating the importation of double-use products and technologies into European Union countries, from non-member countries. (1/4)

➢ We here report a summary table of the levels of limitation to importation, into the European Union, of products connected with cryptography from various countries in the world. The limitation levels are conventionally divided into categories: "Green" involves no restrictions; "Yellow" requires the obtainment of government authorization to importation; "Red" excludes any importation of such products.

Country	Status
Bahrain	Yellow
Belarus	Red
Cambodia	Yellow
Egypt	Yellow
Ghana	Green
Hong Kong	Green/Yellow
Hungary	Green/Yellow
Iran	Yellow

Country	Status
Kazakhstan	Yellow
Latvia	Yellow
Moldova	Yellow
Mongolia	Red
Morocco	Yellow
Myanmar (Burma)	Red
Pakistan	Yellow

Country	Status
Saudi Arabia	Red
Singapore	Green
South Africa	Green/Yellow
South Korea	Yellow
Tunisia	Yellow/Red
Ukraine	Yellow
Vietnam	Yellow

TASCA Law Firm
Legal Advisor

Legal memo - Compatibility of "Criptodynamics" with the norms regulating the importation of double-use products and technologies into European Union countries, from non-member countries. (2/4)

- For the case at hand, we deem it useful to briefly analyze the specifics of a few countries that correspond to potential markets for the activity of our clients, not included in the table reported in consideration of the synopses in the previous page.

China

- In China there are formal policy restrictions regulating import, export, trade and use of cryptographic technology. In December 2009 the State Encryption Management Bureau (SEMB) and the General Administration Customs (GAC) have issued, jointly, the Catalogue for the Administration of Import of Encryption Products and Equipment Containing Encryption Technology (First Batch). The governing body overseeing the release of authorizations, as indicated in the Catalogue, is SEMB. The policies currently in force require, moreover, that the authorization be requested also in case a technological product based on cryptography is not included in the Catalogue.
- Despite the highly restrictive stance of this policy, as of today, it has been consistently disregarded by Chinese business enterprises and government agencies alike.

Russia

- Russian policies appear similar as those applied by China and Israel, requiring the obtainment of licenses for the importation and national use of ciphering products. Unlike the mentioned states, Russia is a participant in the Wassenaar Arrangement. The exportation of cryptographic products out of Russia is generally subject to a license requirement.

TASCA Law Firm
Legal Advisor

Legal memo - Compatibility of "Criptodynamics" with the norms regulating the importation of double-use products and technologies into European Union countries, from non-member countries. (3/4)

USA

- The rules governing the export of cryptographic technology in force today in the United States are moderately restrictive. The technologies based on cryptography with length exceeding 64 bits can now be imported after a simple 30 day examination by the Bureau of Industry and Security – US Department of Commerce (BIS). The same products can be exported to European Union member states and eight additional countries (including Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland, Switzerland), requiring only that their examination be registered with the BIS. A primary role in the commercialization of cryptography is played by the National Security Agency (NSA), which acts as consultant for BIS and the Department of Commerce. Though moderately restrictive, these rules are scrupulously applied by business enterprises and government agencies. Cryptography applications, however, should not encounter any authorization obstacles when exported to the US.

Israel

- The importation and exportation of cryptography requires a license granted by the Director General of the Ministry of Defence, through the assistance of an advisory committee. The Director General may grant a general license to the export of a specific type of cryptography product. The country's policies do not impose specific limits to the length of the key. Licenses are granted on a case-by-case basis. Overall, however, we may define the Israel control system as being highly restrictive with regard to the import/export of cryptography based products.

TASCA Law Firm

Legal memo - Compatibility of "Criptodynamics" with the norms regulating the importation of double-use products and technologies into European Union countries, from non-member countries. (4/4)

India

- India requires an import license for the producers of cryptographic applications. The importation of cryptography software is not subject to any regulatory restrictions.

Brazil

- In Brazil there are no controls connected to the exportation or importation of products of cryptography; Brazil is not a subscriber of the Wassenaar Arrangement.

Canada

- There are no restrictions on the importation or exportation of ciphering products in Canada. The exportation policies in force in Canada appear to be in line with the policies of countries such as the US, UK and Australia, in the sense that Canada's Communications Security Establishment (CSE) cooperates with the corresponding authorities of the mentioned countries.

Australia

- There are no restrictions on the importation and national use of products connected with cryptography, but their exportation is controlled by the Department of Defence, in compliance with the Wassenaar Arrangement.

TASCA Law Firm

Legal memo – Recovery key - key availability (1/4)

- A fundamental issue connected with the use of crypto-dynamic applications in telecommunications (SMS/MMS) is that of guaranteeing the availability of the generated keys, in compliance with the applicable laws.
- In particular, the issue facing the providers of services based cryptographic systems – and, in the case at hand through crypto-dynamic methods in non-voice telecommunication (SMS/MMS) – is that of retaining the information relating to the effected transmissions for specific amounts of time, in order to guarantee the availability of such data for inspections by law enforcement authorities.
- On this last point, we must observe how, within the European Community, a number of regulations seem to overlap: Directive 95/46/EC, on the treatment of personal data; Directive 2002/58/ EC, on the treatment of personal data in electronic communication; Directive 2006/24/EC, which partially modifies the earlier Directive 2002/58/EC, and dictates a specific discipline in the treatment of data by providers of electronic communication services of public access, or public communication networks.
- Such Directives, which do not possess direct application force in single member States, not being self-executing, have caused, in single States, the creation of internal and national implementing laws and regulations, balancing out the varying weights and rankings assigned to legal interests and rights within the European Union.

TASCA Law Firm

Legal Advisor

Legal memo – Recovery key - key availability (2/4)

- As to the activity of providing cryptography services through SMS/MMS communication, the most relevant Directive on the matter is Directive 2006/24/EC.
- At Article 1 its scope of application is thus explained: "*1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. 2. This Directive shall apply to* ***traffic and location data*** *on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user.* ***It shall not apply to the content of electronic communications****, including information consulted using an electronic communications network*".
- The data that needs to be retained, as per Art. 5 of the Directive, are therefore those necessary to trace and identify the source and destination of a communication, concerning access to the Internet, Internet-based electronic mail, Internet- based telephone communication, all the data required to determine the date, time, and duration of a communication, the type of such communication, the tools used to communicate, and the data needed to determine the location of the mobile communication equipment.

TASCA Law Firm
Legal Advisor

Legal memo – Recovery key - key availability (3/4)

- **Nonetheless, such Directive excludes, at Art.5, sub-article 2, the conservation of data concerning the content of communication:** ***"No data revealing the content of the communication may be retained pursuant to this Directive."***
- **This clearly assumes critical, decisive relevance in relation to the applications of Cryptodynamics destined for and applied to non-voice telecommunication (SMS/MMS) and Web-based telecommunication.**
- **Based on Art. 6 of the Directive, furthermore, member States are to cause such categories of data to be retained for periods not less than 6 months and not exceeding 2 years from the date of such communication.**
- Lastly, of particular interest to the case at hand is the provision of Art. 4 of the Directive, which reads that **the procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law**. In Italy, for instance, the Directive was implemented through Legislative Decree No. 109/2008.
- **From the hypotheses thus far discussed, it follows that, within the European Union, a provider of Cryptodynamic services applied to telecommunications shall, in the future, conform to the national regulations implementing Directive 2006/24/EC, already observed by telephone operators.**

Legal memo – Recovery key - key availability (4/4)

- **Our client, asserting to possess the capacity to retain data in compliance with the law, shall be required to retain the cryptography keys (recovery keys) for the period established by the applicable regulations, so as to make them available to any law enforcement authority that might require them.**
- **According to the dispositions of the above-mentioned Art. 5, sub-article 2 of the Directive, there is no law requiring service providers to make available any data relating to the content of communications - and consequently, also the instruments (keys) to decrypt the content of any e-mail, file, or SMS/MMS communication -, that requirement being expressly excluded by the Directive.**
- In conclusion, the unconditionality of the principle of privacy protection, a primary value safeguarded by EU law-makers, releases the providers of Cryptodynamic services applied to telecommunication from the obligation to retain the recovery keys when such keys are generated to encrypt only the content, or better yet, the text, of the telecommunication. Such obligations, in fact, pertain exclusively to data relating to time, location, and identification of users, concerning "non-voice" telephone or electronic transmission (including e-mail or any other type of electronic file). In the case at hand, the keys generated through our client's technology, as it was illustrated and explained to us, are substantially instruments to encrypt "content"; we may thus conclude that such keys appear not to be subject to any law regulating the use of cryptography. Nonetheless, the keys must still be retained in compliance with Directive 2006/24/EC, with regard to the access of data relating to time, location, and identification of the users originating the electronic or telecommunication traffic.

TASCA Law Firm
Legal Advisor

Legal memo – Compatibility of "Cryptodynamics" with eBook publishing

- The commercialization of the Cryptodynamic application to e-Books raises no issues relating to the application of any regulation. A user connecting to the Internet to choose an e-Book to read formulates his request, and, once the transaction is concluded, he has the right to use an electronic channel to browse through the chosen text for the time agreed upon. Such transaction, in the European Union, falls squarely within the scope of policies regulating electronic commerce.
- Such discipline is regulated by Directive 21/2000/EC.
- As to the specific use of cryptographic technology applied to e-Books, with regard to EU policies, Directive 2001/29/EC, at Art. 6, requires each Member State to institute adequate laws to protect against the elusion of effective technologic techniques (such as Cryptodynamics), used by persons acting deliberately, or whose actions may reasonably be considered deliberate, with the purpose of eluding authorship rights (such as in the case of e-Books).
- In other words, the Directive assigns e-Book Authors the possibility to adopt technological measures, such as Cryptodynamics, to prevent the violation of authorship rights.

Studio Legale Tasca

Gaetano Tasca, Attorney at Law