The « trust online » charter.

(automatic translation of an unofficial document
published by the webzine « pcinpact.com »
june 6th, 2008)

The charter "trust online" reflects the government's willingness to make the Internet the most secure environment possible for all citizens. It relies on voluntary providers to take part in the project of building the "civility and security of the Internet."

In line with the charter against « odious products » signed on June 14, 2004, and with the work within the « Forum des Droits sur Internet », the service providers (ISPs and mobile operators, service providers and online publishers) comply with these commitments whatever the legal status of each player on the Internet (notably against the LCEN law).

These commitments are part of an existing legislative and regulatory framework defining the conditions for successful implementation of these texts by actors of the Internet and public authorities, taking into account recent technological developments

The commitments should also comply with the latest recommendations of the Council of Europe adopted at its annual conference OCTOPUS 2008 in April 2008.

Commitments made to users:

I: To enhance the safety of the user:

Last forward by the signatories on their products, home page and through links, information and content relating to:

. Risks security of data and equipment (viruses, spyware, software connection to numbers, piracy connection, secure WiFi ...)
. The technical means available to Internet users to protect them and the need to update

. The advice of good practices existing in order to fight against spam (eg link to Signal Spam)
. information on scams and emerging risks in terms of economic crime on the Internet (spam, phtising, capture credit card number.

Ensuring the security of the equipment:

. Carry out an active approach on the technical risks emerging for the user.
. Establish a proactive security equipment by appropriate measures (such information, suspension, termination, blocking some ports ...) from clients involving network security.
. Reconfigure equipment provided to users so they reach a level of default security that is optimal according to the state of the art. (end page 1)

. The fight against spam through an appropriate policy (filtering, link reporting, application of quotas sending ...) creating an address such as "abuse @" and actively participating in the program SignalSpam.

II. Providing general information

Last forward by the signatories on their products, home page and through links, content relating to:
. The risks of exposure to harmful content and procedure for reporting by providing access links to all platforms existing reporting.
. Issues related to the safeguarding of personal data (minors?)
. The technical means available to Internet users for them.
. A description of parental control software and their evaluations (ISP software and Trade) as well as assistance in the installation and configuration.
. Advice vigilance (eg guide)

III. Oversee the use of services through a charter for users:

Preparation and put forward by the signatories of a charter of the user include:

. The rules of copyright that any content must comply with.
. The behaviour and content permitted or prohibited on the service and recalling the responsibilities involved, notably for minors.
. An awareness and encouragement to moderate Internet content adressed to the creators of forums, blogs ... and information on technical means adequate to do so.
. The requirement for Internet content producers to stop minors from accessing any content within the framework of Article 227-24 of the Penal Code.
. The possibility to forsee, by contract, a form of suspension of the possibility of publishing by persons other than the creator of space, in the absence of any updating, modification, intervention by the moderator of content for three months, and that measures of suspension or removal of space.

Engagement of the customer on its editorial line:

. The interactive spaces for minors are controlled by hand.
. The services and content clearly intended to minors do not contain advertising that promote goods or services inappropriate (eg services meetings adults, tobacco, alcohol ...) or contrary to the recommendation "child" of the BVP.
. The advertising content relating to Article 227-24 of the Penal Code are distributed in areas that "adult" where access to minors is strongly controlled by an effective depending on the state of the art.
. The contents within the framework of Article 227-24 of the Penal Code and hyperlinks pointing to such content are distributed in areas that "adult" where access by minors is strongly controlled by an effective, depending on the state of the art.
. The interactive spaces for adults are subject to control by an effective depending on the state of the art. (end page 2)

IV. Allowing better reporting from the Internet:

Improving procedures for reporting:
. Putting forward a reporting procedure clear, easily understandable and accessible by the Internet user on content produced, distributed or hosted by the signatory.
. Providing a quick response to requests received through this and inform the user on the existence of the contact point of the AFA and platform reporting of the Ministry of Interior)
. To develop internal procedures to respond properly and in conjunction with the competent authorities in reporting cases of content or illicit behaviour.

---> towards labelling

Commitments made to the authorities

V. Participate to reporting policy:

Commitment of the provider on its reporting policy:

. He tells to the authorities, the contents and behaviours that have been notified that may be a legal offense:
the fifth and eighth paragraphs of Article 24 of the Act of 29 July 1881 on freedom of the press (crimes against humanity, war crimes, incitement to racial hatred ...)
and Article 227-23 of the Penal Code. (representation of a minor with a pornographic)

. He also pointed out in the same conditions, the content and conduct showing an immediate risk to the safety of persons and goods. In the latter case, and when it has data that could help identifying the author of the content in question, the provider accompanies the reporting of this information in order to prevent damage to the physical integrity of the person who it was reported.

VI. Improve response time to judicial requisitions:

The signatory is committed to bringing as soon as possible the requisitioning of Justice:
. It strives to permit identification of the holder of an e-mail address after receiving a requisition and the holder of an IP address with the Internet service provider after receiving the document. It strives for requisitions and formal, non-standard requests, to provide an initial response (acknowledgement of receipt, indicating the estimated time of response to the request, etc.).
. It pledges to set up a "service obligations" performance or, if this is not possible, to name a person responsible for processing the responses. These data are regularly updated and communicated to the "one-stop shops" set up by the police and gendarmerie in conjunction with the delegation of judicial interceptions. These authorities are committed to providing an update of the details of such "one-stop shops".

VII. Better participate in the work of public authorities in preserving and transmitting data:
(end page 3)

The provider puts in place, for compliance with laws and regulations, a conservation and transmission of data:
. It keeps all the connection data when those are necessary for the purposes of research, finding and prosecuting criminal offences. It owns and preserves the data likely to enable the identification of anyone who has contributed to the creation of content or any content of services it is providing. These data are stored 1 year.
. In the context of data communication connection, the service provider communicate all elements for identification in his possession, according to the law, allowing the authorities to determine the identity of the user.

VIII. Establish an effective withdrawal and suspension, or blocking certain content:

The signing sets up a procedure for withdrawal and suspension appropriate:
. It pledged to withdraw or suspend promptly content at the request of judicial authorities ousur request.
. Where shall withdraw a content and report it to authorities, the sigantaire proceeded to transmit a copy of the data removed and stored in the original format.
. The signatory agrees to return or restore data in the format in which they appear before the withdrawal or suspension.
. In the case of a child pornography sites, which are reported by the Ministry of the Interior, ISPs undertake what is necessary to block access to those sites through technical means they deem most appropriate. (end page 4).