Benjamin Gittins
Chief Technical Officer
Tel: +356 9944 9390
Fax: +356 2156 2164
cto@pqs.io

Synaptic Laboratories Ltd.
All Correspondence to:
PO BOX 5, Nadur NDR-1000
MALTA, Europe
www.synaptic-labs.com

Monday, 7 June 2010

To: **The National Telecommunications Administration** at
U.S. Department of Commerce, 1401
Constitution Avenue, NW., Room 4725,
Washington, DC 20230.

Re: **Information Privacy and Innovation in the Internet Economy**
Call for public comment

This letter is written in response to the call for public comment made in the [Federal Register: April 23, 2010 (Volume 75, Number 78)], [Page 21226-21231], [Docket No. 100402174-0175-01].

We note the following text from the above call:

> *This Notice of Inquiry seeks comment on the impact of the current privacy framework on Internet commerce and innovation, both from the commercial and consumer perspective, as well as ways in which it may be necessary to adjust today's privacy framework to preserve and even enhance innovation and privacy in our new web-centric information environment. The questions below are intended to assist in framing the issues and* ***should not*** *be construed as a limitation on comments that parties may submit.* ***The Department invites comment on the full range of issues that may be presented by this inquiry.***

Thank you for making this important call for public comment. We would like to respond to this call by providing 6 files of input in 3 bundles. The title of the 6 files is as follows:

INPUT 1) http://www.think-trust.eu/downloads/public-documents/deliverabled3-1a/download.html
INPUT 2) http://www.think-trust.eu/downloads/public-documents/d3-1b/download.html
INPUT 3) "Part 4: The need for the EC to fund the development of an electronic requirements management process to support the conversion of existing standards, existing policy guidelines and existing laws of several nations simultaneously in a unified requirements model that also supports national and regional variations."
INPUT 4) "Part 5: A) The need to evaluate the effectiveness of data depersonalisation techniques and it's impact on the community; and B) Measuring the wider impacts of unauthorised information."
INPUT 5) "Part 6: A) Privacy Enhancing Technologies should be explicitly rejected if they act as a legitimising facade behind which long-lived privacy invasion and political oppression could be deployed by (present or future) Governments, and B) We recommend that there is a need to explicitly require all stake-holders to be equally accountable in all information processing and security systems."
INPUT 6) "Synaptic Laboratory Limited's Submission Responding to ENISA's Call for Scenario Proposals on Emerging and Future Risks"

Before describing Synaptic's input, I would like to provide some context.

Synaptic Laboratories is a **micro** Private Technology Company managed by Australian citizens with Directors in Gozo, Malta (Europe) and Australia. We are operating internationally on a 'virtual' basis with ten years of completed cross domain research and design. Our core business is cutting edge cyber security solutions for Today's Internet (and the Future Internet).

We are active in the US Federal Cybersecurity initiatives:

- having made submissions to the NITRD Cyber Leap year public Requests for Input[1]
- having participated at the 'by invitation' NITRD Cyber Leap Year Summit where 6 of our proposals were carried forward in the Participants Ideas Report[2]
- having presented further information on these proposals[3] at the peer reviewed Oak Ridge National Laboratory 6th Annual Cyber Security and Information Intelligence Workshop (CSIIRW)[4] held in April 2010 and also at the IEEE Key Management Summit held in May 2010, where we were a sponsor[5].

Specifically Synaptic Labs are focussing on Global-scale Identity Management and Cryptographic Key Management (IdM/CKM) along the lines called for by the U.S. Department of Homeland Security in their Nov. 2009 "*A Roadmap for Cybersecurity Research*" publication[6], and on next generation Internet protocols with privacy enhancing features as published in the NITRD NCLY 2009 Participants Report[7].

Synaptic Labs was one of the few foreign participants invited to the NITRD National Cyber Leap Year Summit, and we have been acting as a bridge between US and European Government Level security initiatives, seeking to bring to the attention of the other overlapping initiatives where synchronisation and international normalisation may be possible.

Synaptic Labs has made submissions to European Calls that correspond with or are the equivalent in most regards with the subjects of your Call. Unfortunately, due to work pressures and lack of time we are unable to repackage our European submissions to specifically address your Call, however we are forwarding now copies of our European submissions trusting that you will easily find the content relevant or your purposes. We have previously forwarded at least one of these submissions to our contacts at NIST and Miles Smid (Orion Security, formerly at NIST) had this to say [quoted with permission]:

> *"I think that this is an interesting idea and indicates how standards requirements will need to be managed in the future."*

---

[1] http://synaptic-labs.com/resources/synaptic-publications/104-input-to-ec-and-us-funded-ict-initiatives/348-pub-synaptic-labs-3-inputs-to-nitrds-call-for-qleap-aheadq-ideas-2009.html

[2] http://synaptic-labs.com/resources/security-bibliography/105-security-organisations-projects-and-calls/331-bibliography-us-nitrd-ncly-security-summit-2009.html

[3] http://synaptic-labs.com/resources/security-bibliography/106-security-conferences/340-bibliography-us-ornl-csiirw-6-2010.html

[4] http://www.csiir.ornl.gov/csiirw/10/index.html

[5] http://2010.keymanagementsummit.org/ and http://storageconference.org/2010/Presentations.html#KMS

[6] http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

[7] See our extracts from this report here: http://media.pqs.io/pub/papers/NCLY/20091115-NCLY-Summit2009-Participants_Ideas_Report-Extracts.pdf

SYNAPTIC LABS' FIRST BUNDLE OF INPUT INTO YOUR CALL

The first bundle we are providing is simply a copy of the deliverables from a European Commission funded project that we expect you will already be aware of, but just in case, we provide them now. The project we refer to is called Think-Trust[8] and it was tasked with issuing a Call for public input on very similar subject matters as your Call. These deliverables are available to the public and we believe you will find them relevant and of interest. Synaptic Labs actually made extensive inputs to this European project (See second bundle below).

Think-Trust (FP7-216890) is a project funded by the European Commission's 7th Framework Information Society Technologies (IST) Programme, within the Unit F5 ICT for Trust and Security. It is investigating Trust, Security, Dependability, Privacy and Identity from ICT and Societal Perspectives. Think-Trust is a Co-ordination Action (CA) project. It started on January 1st 2008, receives funding of 580,000 Euro and has a 30-month duration.

Think-Trust produced a list of research challenges which need to be addressed to work towards a trustworthy ICT environment. Think-Trust's deliverables make comment on a wide range of issues on information privacy and the Internet and these, in our opinion, directly relate to your call on "Information Privacy and Innovation in the Internet Economy".

In this letter, Synaptic submits the Think-Trust's two deliverables D3.1A and D3.1B **as input into your process.** Please find the two documents freely available for download here:

> **INPUT 1)** http://www.think-trust.eu/downloads/public-documents/deliverabled3-1a/download.html
> **INPUT 2)** http://www.think-trust.eu/downloads/public-documents/d3-1b/download.html

SYNAPTIC'S SECOND BUNDLE OF INPUT INTO YOUR CALL

As previously mentioned, Synaptic Laboratories is a MICRO research and design company. We are actively participating in US and EU security initiatives, however our resources are inherently constrained.

We kindly ask for your understanding with regard to our second bundle of input. We have thoughtfully selected a subset of 3 out of our 6 submissions to THINK-TRUST's D3.1A and D3.1B call **unmodified**. We have carefully chosen these submissions as they are most relevant to your call.

We ask the "Information Privacy and Innovation in the Internet Economy" study group to kindly consider the CONTENT of the arguments found in these publications on their own merit, in respect to your activities, even though they are not framed directly in response to your call. We note that our submissions to Think-Trust made extensive reference to US Federal Initiatives and possible areas of international overlap.

Please find the three documents, **as input into your process:**

INPUT 3) "Part 4: The need for the EC to fund the development of an electronic requirements management process to support the conversion of existing standards, existing policy guidelines and existing laws of several nations simultaneously in a unified requirements model that also supports national and regional variations."

> (Also available at: http://media.pqs.io/pub/papers/TT/20100127-TT-D3-1b-P4.pdf)
>
> **Relevance**: As noted in your call "*Small and medium-sized entities (SMEs) and startup companies face the same data protection laws and guidelines as their larger counterparts, but with fewer resources.*" This proposal suggests that relevant privacy laws, national and international, such be unified in an electronic requirement model, enabling small organisations to quickly identify what

[8] http://www.think-trust.eu/

requirements they must satisfy in their software and business processes. Many other benefits are outlined.

Miles Smid (of Orion Security, formerly of NIST) had this to say about this proposal:

> *"I think that this is an interesting idea and indicates how standards requirements will need to be managed in the future."*

INPUT 4) "Part 5: A) The need to evaluate the effectiveness of data depersonalisation techniques and it's impact on the community; and B) Measuring the wider impacts of unauthorised information."

(Also available at: http://media.pqs.io/pub/papers/TT/20100128-TT-D3-1b-P5.pdf)

Relevance: Your call asks for information on data depersonalisation and re-identification technologies. This is excellent. In section A) we propose that a formal Government level study is required to evaluate the state-of-the-art, study the behaviour of the market in using depersonalised data, and to use that data to set guidelines and best practices. In section B) we call for a study to measure the cost of unauthorised information disclosure. This information is required to help establish "appropriate levels" of security protection appropriate to the damage of privacy exposure to the relevant stake holder(s).

INPUT 5) "Part 6: A) Privacy Enhancing Technologies should be explicitly rejected if they act as a legitimising facade behind which long-lived privacy invasion and political oppression could be deployed by (present or future) Governments, and B) We recommend that there is a need to explicitly require all stake-holders to be equally accountable in all information processing and security systems."

(Also available at: http://media.pqs.io/pub/papers/TT/20100129-TT-D3-1b-P6.pdf)

Relevance: Your call asks for information on New Privacy-Enhancing Technologies and Information Management Processes. This is excellent. As you are no doubt already aware, the EU is a strong proponent for privacy-enhancing technologies. In section A of part 6 of our input to Think-Trust we draw out a point that certain privacy enhancing technologies should be rejected if that proposal acts as a legitimising facade behind which long-lived privacy invasion and political oppression could be deployed. In section B, we take a broader look at privacy and accountability in security systems and observe that there is a need to explicitly require all stake-holders to be equally accountable and protected in all information processing and security systems.

SYNAPTIC'S THIRD BUNDLE OF INPUT INTO YOUR CALL

Another European organisation Synaptic has participated with is ENISA.

The European Network and Information Security Agency (ENISA) is an agency of the European Union. ENISA was created in 2004 by EU Regulation No 460/2004 and is fully operational since September 1st, 2005. The objective of ENISA is to improve network and information security in the European Union. The agency has to contribute to the development of a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, and consequently will contribute to the smooth functioning of the EU Internal Market.

In 2009-2010 the European Network and Information Security Agency (ENISA) www.enisa.europa.eu made a call for **Scenario Proposals on Emerging and Future Risks**.

Synaptic Labs' proposal to ENISA was selected for study in 2010 in the area of Trust and Privacy. In this area ENISA was looking for proposals to identify major risks in the area of trust, security and **privacy** posed by new and emerging technologies and applications. ENISA restricted scenario proposals from including proprietary technologies, and we complied with this restriction. Synaptic participated in this Call with a scenario focused on the risks associated with the global dependency upon Public Key Cryptography (PKC)

and Public Key Infrastructure (PKI). Synaptic's publication outlined **90 different threats and issues** under 8 headings identified within the submission. It has a 3 page executive summary and a further 56-page supporting document including extensive references.

This publication touches on the **known** future risks of widely anticipated **complete privacy failure** due to continued use of public key technologies (on account of Peter Shor's Quantum Algorithms and their derivatives), issues of single point of trust failure in the civilian certificate authority that **allow identity fraud** to be performed (which can **result in privacy loss**), and also raises serious concerns of **data ownership and personal control over biometric data** which is traded internationally (and protected using known at risk Public Key Technologies).

Our publication outlines how these issues collectively **impact the individuals' fundamental rights** and opportunities for development in the community. It also shows how this negatively impacts the public interest because **self-determination is a necessary condition for the functionality of a liberal democratic polity** which is based on its citizens' ability to act and to participate.

Please find the following document, **as input into your process:**

INPUT 6) "Synaptic Laboratory Limited's Submission Responding to ENISA's Call for Scenario Proposals on Emerging and Future Risks"

(Also available at: http://media.pqs.io/pub/papers/ENISA/20100330-ENISA-FR-Synaptic.pdf)

Thank you again for a) making the call for input and b) for your understanding in our resource constraints that have limited our ability to re-frame our input specifically to your process.

Yours sincerely,

Benjamin Gittins

Chief Technical Officer
Synaptic Laboratories Limited
June 4, 2010