Ronald Kelson
Chairperson and CEO
Tel: +356 7956 2164
Fax: +356 2156 2164
ceo@pqs.io

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

Friday, 29 January 2010

PART 6 OF SYNAPTIC LABORATORIES LIMITED INPUT TO THINK-TRUST's CONSULTATION ON THEIR DRAFT "D3.1B RECOMMENDATIONS REPORT" TO THE EUROPEAN COMMISSION

Privacy Enhancing Technologies should be explicitly rejected if they act as a legitimizing facade behind which long-lived privacy invasion and political oppression could be deployed by (present or future) Governments;

We recommend that a Global PET solution should be explicitly designed to pro-actively prevent abuse by Governments or Regions;

and

We recommend that there is a need to explicitly require all stake-holders to be equally accountable in all information processing and security systems.

1. Escrow and Data Retention

In section 4.4 on Accountability, the Think-Trust deliverable D3.1B discusses:

> **"Delegation, proxy, anonymity management"** and
> **"Anonymous/pseudonymous charging and payment systems".**

Section 4.4 also states:

> **"By partially moving system control towards establishing data either *a priori* or *a posteriori*, these two approaches are likely to considerably diminish or at least reduce the need for risky recourse to cumbersome identification methods through permanent and intrusive monitoring of all data flows."**

Synaptic is concerned that Think-Trust may be proposing the design of Privacy Enhancing Technologies that:

- embeds global identity information with each "data flow" in a way that permits escrow functionality such that "data either *a priori* or *a posteriori*" can be recovered; and/or
- creation of systems that "mass archive" potentially interesting information in a way that permits the identity of the parties and the cleartext to be recovered either *a priori* or *a posteriori*.

Synaptic strongly recommends that Privacy Enhancing Technologies should be explicitly rejected by Think-Trust when and if they act as a legitimising facade behind which long-lived privacy invasion and political oppression could be deployed by (present or future) Governments.

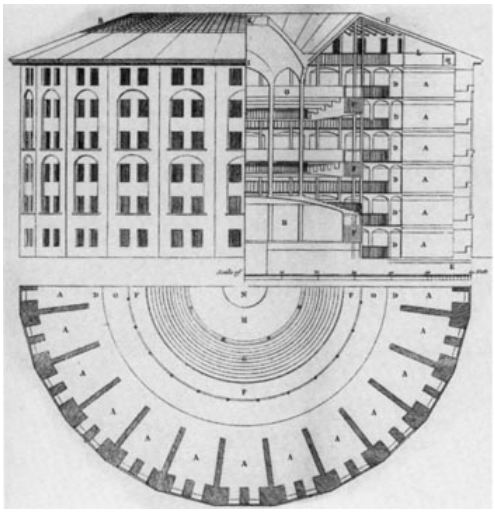
> "At a crypto conference when Clipper was hot, I was approached by Birgit Pfitzmann, a German cryptographer with a very compelling statement that moved me greatly. *'Brian, America is very fortunate, you have never had a truly evil Government. Perhaps corrupt, perhaps inept, but never truly evil. We in Europe have not been so fortunate. I trust the Government I have today, but I will not give it power over me that I would not trust in the hands of a future Government I would not trust.' And I agree with her.*"
> – Brian Snow, former Technical Director of the information assurance directorate of the NSA, 2006

The Clipper Chip is a cryptographic device intended to protect private communications while at the same time permitting government agents to obtain the "keys" upon presentation of "legal authorization."

If a Government is permitted the CAPABILITY to employ centralized escrow measures on all security systems in the name of "accountability" within its jurisdiction, this would fundamentally undermine trust and create the perception – if not the reality of – a panopticon, and open potential for real abuse of the captured and permanently archived data.

The concept of the original panopticon design (illustrated to the right for use as a prison) is to allow an observer to observe (-opticon) all (pan-) prisoners without the prisoners being able to tell whether they are being watched, thereby conveying what one architect has called the "sentiment of an invisible omniscience."

There is a real concern that all sensitive data might be *a priori* or *a posteriori* exposed in a way that the sending and receiving parties cannot ascertain, audit or control.



> *"Whoever is **uncertain if divergent kinds of behavior will be recorded at any time and this information will be stored permanently, used or passed on**, will try not to attract attention by these kinds of behavior. Whoever expects that e.g. the attendance of an assembly or the participation in a civic action group will be registered by the authorities and that this will probably cause risks, may probably abandon their corresponding fundamental rights (Art. 8, 9 GG). This would not only impact the individuals' chances for development but also 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."*
>
> *– from the German Federal Constitutional Court census judgment of 1983 as quoted in the article "Current Legal Issues on Video Surveillance" contributed to the SECURITY Congress 2000, Oct. 9-12, 2000 in Essen by Dr Thilo Weichert.*

Synaptic asks how can Government controlled pseudo-anonymity protect the civilian from potential abuses within the current, or future Government?

The paranoid members of our community would probably be correct in fearing that citizens using pseudo-anonymity would be flagging themselves for special attention by their secret Government security organisations.

It would be reasonable to assume that in many cases Government Security Organisations (under the flag of national security) would be able to monitor all Government 'certified secure' channels in exactly the same way, and with the same impunity and lack of external oversight, they are doing already over unsecured communication paths.

Of course if a Government chose to maintain escrow access to sensitive personal and corporate data then the question becomes one of security of the data thus obtained. Governments have a questionable record of holding secure their own records and systems, much less confidential data they accumulate on the general public.

Furthermore, the complexities of international stability are increased as a result of potential international espionage, even between EU member states.

See Part 3 of our input to the Think-Trust D3.1b consultation process for more information on the importance of end-to-end redundancy, no single points of potential failure and separation of powers.

2. The need for legalized interception systems to be cryptographically secure

According to a review by the well known American cryptographer Matt Blaze and 4 co-authors, a real problem that exists in the USA today is that the American wiretap protocols -- used in the most serious criminal investigations -- were apparently designed and deployed (and mandated in virtually every communications switch in the US) without first subjecting them to a meaningful security analysis.

According to Matt Blaze current US Legalised Interception systems were engineered to work well in the average case, but ignored the worst case of an adversary trying to create conditions unfavorable to the eavesdropper. And as the services for which these protocols are used have expanded, they've created a wider range of edge conditions, with more opportunities for manipulation and mischief.

See their paper, Can They Hear Me Now? A Security Analysis of Law Enforcement Wiretaps[1] which examines the standard "lawful access" protocols used to deliver intercepted telephone (and some Internet) traffic to US law enforcement agencies.

— It is conceivable that a similar situation exists in European States.

If wiretaping and escrow systems are going to be built, then we propose that they must be engineered at the same levels of auditability, robustness and security as National Security Systems and with the same accountability and privacy controls required in Enterprise systems by European Data Privacy Directives.

[1] http://www.crypto.com/papers/calea-ccs2009.pdf

3. Current interception systems put the community at risk

We extensively quote an article by highly respected cryptographer Bruce Schneier published on CNN[2]:

> **U.S. enables Chinese hacking of Google**
> **January 23, 2010**
>
> Google made headlines when it went public with the fact that Chinese hackers had penetrated some of its services, such as Gmail, in a politically motivated attempt at intelligence gathering. The news here isn't that Chinese hackers engage in these activities or that their attempts are technically sophisticated -- we knew that already -- **it's that the U.S. government inadvertently aided the hackers**.
>
> In order to comply with government search warrants on user data, Google[3] created a backdoor access system into Gmail accounts. This feature is what the Chinese hackers exploited to gain access.
>
> Google's system isn't unique. Democratic governments around the world -- in Sweden[4], Canada[5] and the UK[6], for example -- are rushing to pass laws giving their police new powers of Internet surveillance, in many cases requiring communications system providers to redesign products and services they sell.
>
> Many are also passing data retention laws, forcing companies to retain information on their customers. In the U.S., the 1994 Communications Assistance for Law Enforcement Act required phone companies to facilitate FBI eavesdropping, and since 2001, the National Security Agency has built substantial eavesdropping systems with the help of those phone companies.
>
> Systems like these invite misuse: criminal appropriation, government abuse and stretching by everyone possible to apply to situations that are applicable only by the most tortuous logic. The FBI illegally wiretapped[7] the phones of Americans, often falsely invoking terrorism emergencies, 3,500 times between 2002 and 2006 without a warrant. Internet surveillance and control will be no different.
> …
> China's hackers subverted the access system Google put in place to comply with U.S. intercept orders. **Why does anyone think criminals won't be able to use the same system** to steal bank account and credit card information, use it to launch other attacks or turn it into a massive spam-sending network? Why does anyone think that only authorized law enforcement can mine collected Internet data or eavesdrop on phone and IM conversations?
> ...
> These risks are not merely theoretical. After September 11, the NSA built a surveillance infrastructure to eavesdrop on telephone calls and e-mails within the U.S. **Although procedural rules stated that only non-Americans and international phone calls were to be listened to, actual practice didn't match those rules.** NSA analysts collected[8] more data than they were authorized to and used the system to spy on wives, girlfriends and notables such as President Clinton[9].
>
> But that's not the most serious misuse of a telecommunications surveillance infrastructure. In Greece, between June 2004 and March 2005, someone wiretapped more than 100 cell phones belonging to members of the Greek government: the prime minister and the ministers of defense, foreign affairs and justice.
>
> Ericsson built this wiretapping capability into Vodafone's products and enabled it only for governments that requested it. Greece wasn't one of those governments, but someone still unknown -- A rival political party? Organized crime? Foreign intelligence? -- figured out how to surreptitiously turn the feature on.

---

[2] http://edition.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html

[3] http://topics.edition.cnn.com/topics/Google_Inc

[4] http://www.thelocal.se/12334/20080610/

[5] http://www.canada.com/Technology/Feds+give+cops+Internet+snooping+powers/1706191/story.html

[6] http://www.theregister.co.uk/2008/05/20/central_government_database_proposed/

[7] http://www.nytimes.com/2010/01/21/us/21fbi.html

[8] http://www.nytimes.com/2009/04/16/us/16nsa.html?_r=1

[9] http://www.wired.com/threatlevel/2009/06/pinwale

> **And surveillance infrastructure can be exported, which also aids totalitarianism around the world.** Western companies[10] like Siemens and Nokia built Iran's surveillance. U.S. companies helped[11] build China's electronic police state. Just last year, Twitter's anonymity saved the lives of Iranian dissidents, anonymity that many governments want to eliminate.
>
> In the aftermath of Google's announcement, some members of Congress are reviving a bill[12] banning U.S. tech companies from working with governments that digitally spy on their citizens. Presumably, those legislators don't understand that their own government is on the list.
>
> The problem is that such control makes us all less safe. Whether the eavesdroppers are the good guys or the bad guys, these systems put us all at greater risk. Communications systems that have no inherent eavesdropping capabilities are more secure than systems with those capabilities built in. And it's bad civic hygiene to build technologies that could someday be used to facilitate a police state.

With regard to the question posed by Think-Trust in section 4.10 of T-T D3.1b:

> *"Is it more cost-effective to prevent a data breach or just address the consequent damage when one occurs?"*

Synaptic rhetorically asks: How can we measure the damage of data breaches to human rights activists in China?

4. Equal Accountability Inside Security Systems

It is not sufficient to say, "Enterprises must behave in this proper way by law", and then not impose functionally equivalent requirements on ALL branches of Government.

Historically Accountability, Transparency, Systems of Checks and Balances, and Separation of Powers have been the founding principles of democratic institutions. The Spirit of Laws (French: L'esprit des lois) is a treatise on political theory **first published anonymously** by Charles de Secondat, Baron de Montesquieu[13] in 1748 that covers a wide range of topics in politics, the law, sociology, and anthropology. In this political treatise Montesquieu advocates constitutionalism and the separation of powers, the preservation of civil liberties and the rule of law, and the idea that political and legal institutions ought to reflect the social and geographical character of each particular community. All these fundamental principles remain as valid today as they did in 1748.

It is these principles that has led to the design of Governments that permit individual citizens of limited means to have some level of trust in the integrity of their Governing system.

The **separation of powers**, **checks-and-balances and the rule of law** should not be an option but a legal requirement in cyber-security systems or electronic law-enforcement activities particularly as it is clearly acknowledged that cyberspace touches every citizen.

Furthermore, it is not sufficient to say that security mechanisms must be in place by law for one group, if some of the mechanisms that are put in place effectively shift liability away from the largest stake holder, or make that large stake holder less accountable than others. This practice is already far to common:

> "The conventional wisdom is that security priorities should be set by risk analysis. However, reality is subtly different: many computer security systems are at least as much about shedding liability as about minimising risk. Banks use computer security mechanisms to transfer liability to their customers; companies use them to transfer liability to their insurers, or (via the public prosecutor) to the taxpayer; and they are also used to shift the blame to other departments ('we did everything that GCHQ told us to')."
> -- Ross J Anderson[14], UK Cryptographer,

---

[10] http://news.bbc.co.uk/2/hi/technology/8112550.stm

[11] http://www.rollingstone.com/politics/story/20797485/chinas_allseeing_eye/print

[12] http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/01/16/BU151BIO84.DTL

[13] http://en.wikipedia.org/wiki/Charles_de_Secondat,_Baron_de_Montesquieu

[14] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.27.4524

Synaptic recommends that a research subject would be to consider in what way legal policies can guide the design and implementation of all information processing and all monitoring systems so that all stake holders can be held externally accountable without exception.

For example laws that:

- stipulate that information processing and monitoring systems must hold ALL stake-holders equally accountable to each other;
- require information processing and monitoring systems to protect the legitimate interest of all stake-holders (and not just the interest of the share-holders);
- require that a stake holder must be readily informed of all actions (including security actions/investigations) taken against their personal sensitive data (even if this might be delayed by some small fixed amount of time, such as maximum 6 to 12 months) - including how this information will be used, and how long it will be retained, and how they can seek redress; and
- require that accountability of internationally deployed information processing and monitoring systems must not be shifted completely away from the users jurisdiction and also must not be constrained to any singular national body.

To provide further support to this argument, let us first consider the Elysée Scandal—named after the palace where the late President Francois Mitterrand set up an undercover listening room. Mitterrand's operatives tapped the calls of his political enemies: lawyers, businessmen, journalists, and even the actress and Chanel model Carole Bouquet. This took place in the mid-1980s but only surfaced recently, and 12 conspirators were brought to trial[15]. **What's interesting—and disturbing—about the Elysée Scandal is that at the time, French authorities had justified the surveillance as a necessary tool to fight terrorism.** This type of action should be detectable near real-time, not several years later after the event, after the damage has been done.

To quote the Wired magazine article that goes into more detail on the illegal wiretapping by the FBI:

> An internal audit found that the (US) FBI broke the law thousands of times when requesting American' pone records using fake emergency letters that were never followed up on with true subpoenas – even though top officials knew the practice was illegal, according to The Washington Post.
> …
> "What is new in the Post's reporting today is that it was FBI supervisors and senior officials who were abusing the system," said Greg Nojeim, a lawyer at the Center for Democracy and Technology.
>
> "The FBI has been assuring us for years that the abuses of the Patriot Act could be cured by more layers of internal review, but now we learn that the supervisors themselves were abusing the process," Nojeim said. **"When people are under pressure, internal review is not enough, there needs to be external oversight, and the best way to do that is to have a judge look at the situation."**
>
> - Ryan Singel, Wired Magazine, Jan 19, 2010

Synaptic argues that Europe's exceptional rules for enforcing data privacy and accountability at the commercial level should also be applied in all information processing systems, including monitoring systems, created for Governments.

Again we argue that accountability of such systems MUST transcend a singular national body, because national Judges are likely to feel the same National pressures that the national security organisations feel.

[15] http://www.time.com/time/magazine/article/0,9171,1027463,00.html

5. The research agendas and systems designed by the EU should be considered for how they influence other nations

The United States and the European Union both proclaim themselves as pillars of democracy to the international community.

As standards of democracy, how they behave has some influence on the behavior of all other Nations.

The research agendas, and the Identity and IT systems proposed by the European Union will also set the next "high water mark" for the behavior of other Governments internationally, particularly as we now live in a globally interdependent and interconnected world village.

The expectations of the common person in the global community will be influenced by the research and development agendas, and security systems built by Europe.

We quote Brian Gladman, a respected cryptographer who has extensive experience working in the UK MoD[16]:

> "Although many democratic countries have institutions and approaches that can significantly limit and control government abuse of key escrow capabilities, **this is not more generally true and in many countries these would undoubtedly be used as a means of oppression.** If democratic countries implement such measures they then have no moral or ethical basis on which to deny these facilities to governments that will use them against their own citizens.
>
> **The ability of encryption to allow people to interact with each other on a global scale without fear of oppression by their governments is just about the most potent capability mankind has had for advancing democracy and human freedom on a global scale.** I consider it a tragedy that the United States in particular, with its strong tradition of promoting democracy and human freedom, should be seeking to deny this technology to those who most need it."

END

[16] http://gladman.plushost.co.uk/oldsite/career/index.php

6. Synaptic's recommendations to Think-Trust

Synaptic is concerned that Think-Trust may be proposing or be thought to be proposing the design of Privacy Enhancing Technologies that could be adapted to operate as centralized monitoring systems.

Synaptic strongly recommends D3.1B explicitly rejected Privacy Enhancing Technologies when they could act as a legitimising facade behind which long-lived privacy invasion and political oppression could be deployed by (present or future) Governments.

Synaptic argues that if D3.1B supports the design of wiretaping and escrow systems then Think-Trust should assert that they must be engineered at the same levels of auditability, robustness and security as National Security Systems and with the same accountability and privacy controls required in Enterprise systems by European Data Privacy Directives to protect the citizen and to free the international community from the existing risks of uncontrolled politically motivated abuse and to prevent the growth of totalitarian states.

Furthermore, synaptic strongly recommends D3.1B explicitly recommend that existing "legalized interception" systems to be studied for their cryptographic security and if they must continue recommend that they:

- have inbuilt end-to-end redundancy;
- are free of single points of potential catastrophic failure;
- distribute trust and separate powers management across multiple autonomous security authorities and nation states;
- permit international external oversight to identify and a legal framework that ensures abuses are corrected and agents held accountable.

Synaptic recommends that a research subject would be to consider in what way legal policies can guide the design and implementation of ALL information technology security systems that hold all stake holders externally accountable without exception.

For example laws that:

- stipulate that information processing and monitoring systems must hold ALL stake-holders equally accountable to each other;
- require information processing and monitoring systems to protect the legitimate interest of all stake-holders (and not just the interest of the share-holders);
- require that a stake holder must be readily informed of all actions (including security actions/investigations) taken against their personal sensitive data (even if this might be delayed by some small fixed amount of time, such as maximum 6 to 12 months) - including how this information will be used, and how long it will be retained, and how they can seek redress; and
- require that accountability of internationally deployed information processing and monitoring systems must not be shifted completely away from the users jurisdiction and also must not be constrained to any singular national body.

About Think-Trust

Think-Trust (T-T) (www.think-trust.eu/) is an F5 Coordination Action under Framework Program 7 (FP7) Challenge 1, Objective ICT-2007.1.4 – Secure, Dependable and Trusted Infrastructures. T-T has been allocated the task of helping to coordinate the response to the needs of a trustworthy ICT future in Europe, through working groups, surveys and consultations resulting in Reports with recommendations and priorities about what needs to be done. Its target audience is the European Commission and policy-makers responsible for future direction, strategies, and priorities for European ICT. T-T deliverables complement the RISEPTIS (Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society [17]) work by providing feedback on priorities based upon input from their various activities and input from the perspective of participants in the European ICT Framework Programme. T-T has completed and published a Report entitled "Recommendations Report" D3.1a [18] and has provided to Synaptic Laboratories Limited a draft of D3.1b for our input prior to its publication. This document forms Part 1 of Synaptic Laboratories Limited input to D3.1b.

About Synaptic Laboratories Limited

Synaptic Laboratories Limited is developing the next generation of secure communications products and protocols to protect global communication networks. Synaptic is guided by a vision of "Long term, high-assurance global data security for all stake-holders".

Synaptic drives data security through the development of innovative security technologies founded on well studied cryptographic techniques. Synaptic can be found on the Web at http://synaptic-labs.com

The Synaptic CTO has been the guest speaker on post quantum security **without the use of quantum cryptography** for three consecutive years at the World Smartcard and Electronic Identification Congress CARTES held each year in Paris, FRANCE.

Synaptic responded with three submissions to the public calls for new 'leap ahead' cybersecurity proposals issued by the US Government's Networking and Information Technology Research and Development Program (NITRD).

Consequently Synaptic Laboratories CTO was formally invited to attend their 'closed' by invitation only' National Cyber Leap Year Summit. The Summit brought together government, industry and academia including the USA's leading innovators to identify requirements and proposals for next generation cyber security solutions. Several Synaptic proposals were taken forward at the Summit. At this Summit Synaptic also actively promoted SecureIST and ThinkTrust deliverables, and consequently Think-Trust is referenced by name along with Synaptic authored proposals in the Summit Participants Idea Report. This Report has been fed as input into the US Administration's cybersecurity planning. More on the Synaptic participation in the US Cybersecurity Initiatives can be found here[19].

Through its participation in US cybersecurity initiatives Synaptic Laboratories Ltd. acts as a bridge to promote European ICT research and planning projects, such as Think-Trust, to an extensive and influential audience in the USA. At the same time we seek to promote the US cybersecurity initiatives and their outcomes in Europe at every opportunity, for example in our presentations at the CARTES World Congress. Our objective is to encourage and accelerate international collaboration in cybersecuriy initiatives with a focus upon globally scalable identity management and cryptographic key management that offers long term assurance (without requiring the use of quantum cryptography) even into the quantum future.

---

[17] http://www.think-trust.eu/riseptis.html

[18] http://www.think-trust.eu/downloads/public-documents/deliverabled3-1a/download.html

[19] http://media.synaptic-labs.com/downloads/pub/publications/NCLY/20091115-NCLY-Summit2009-Participants_Ideas_Report-Extracts.pdf