SYNAPTIC
LABORATORIES LTD.

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, 28 January 2011

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

privacynoi2010@ntia.doc.gov

Re: Cybersecurity, Innovation and the Internet Economy
Notice of Inquiry

This letter is written in response to the notice for inquiry made in the [Federal Register: Dec 21, 2010 (Volume 75, Number 244)], [Page 80042], [Docket No. 101214614-0614-01].

Thank you for making this important call for public comment.

There are seven sections in our reply. We begin with praise for the DoC IPTF and the IPTF Privacy Green Paper, which we consider to be a very valuable contribution and effort. Second, we point to specific sections of that text that we think are highly desirable. Third, we provide some constructive feedback on statements found in the body of the green paper. Four, we make some observations on the DHS fair information practice principles (FIPP). Five, we provide answers to selected questions out of your notice of inquiry. Six, we make a few very minor observations on a few sentences in the text. Seven, we finish with some suggestions regarding a) unique requirements to support small business needs and b) a proposition to survey the community to establish a baseline expectation for data privacy.

We appreciate this opportunity to provide feed back on the UPTF Privacy Green Paper. Should it be helpful, we are at your disposal to provide further clarification on any point we have raised.

Thank you and best regards,

Benjamin GITTINS, on behalf of the Synaptic Laboratories Team.

Table of Contents

About Synaptic Laboratories

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 more than ten years of completed research and design. Our core business is cutting edge cross domain research and design for the cloud, today's Internet and the Future Internet. In recognition of the known interdependencies, our proposals offer a holistic response to a wide range of the hard open problems identified in recent calls by Agencies such as DHS, NIST and NITRD. We offer cross domain proposals for new trustworthy and dependable global-scale identity management, cryptographic key management, cloud computing and Future Internet. None are isolated point solutions. For more information on the specific Agency Calls addressed, and to rapidly appreciate the scope and interplay between our designs, please see our Projects Map when you visit: http://www.ictgozomalta.eu/vision-and-projects/introduction-and-overview-map.html .

We are/were active in various EU and US Federal Cyber Security initiatives, such as NITRD NCLY, NIST CKMS Project, ORNL CSIIRW-6, and IEEE KMS. I was one of the few foreign participants invited to the NITRD National Cyber Leap Year Summit, where six of our proposals were accepted for publication. We frequently act as an information conduit between EU and USA cyber security and related initiatives. We also submitted feedback to the previous NTIA. Please visit our company website http://www.synaptic-labs.com for more information on our activities in the US and the EU.

1. Praise for the DoC IPTF and the IPTF Privacy Green Paper

We affirm that the Department of Commerce Internet Privacy Task Force goals are extremely important to the United States and the global community. Consumer trust and the expectation that personal information that is collected will be used consistently with clearly stated purposes and protected from misuse is indeed fundamental to commercial activities on the Internet.

In fact, we would go further and say that consumer trust requires that organisations use consumer information in a way that protects the legitimate interests of that consumer first, before their own interests.

There appears to be a wide international consensus that an erosion of trust in information-processing, and services provided over the Internet in general, will inhibit the adoption of new technologies. For example, the October 2009 E.U. THINK-TRUST RISEPTIS Report[1] entitled "Trust in the information society", asserts that "*The trustworthiness of our increasingly digitised world is at stake.*" Furthermore: *"if citizens feel threatened, mistrustful and increasingly hesitant towards innovative applications and services, our whole society may end up being the loser.*"

The 5 key recommendations made in 4 broad categories that make up the "Dynamic Policy Framework" approach appear sound and well considered. We feel that they could lead to significant improvements in the ability for organisations, both large and small, to navigate the complexity of international privacy laws while also seeking to improve customer privacy in practice.

On reading the green-paper, it was quite clear that content was developed through an inclusive, collaborative, and considered process. We feel it successfully presents a balanced overview of the privacy concerns of the various category of stakeholders. We did not perceive imbalance or undue bias in how the legitimate fears, concerns and recommendations of various parties were presented.

We concur with the statement that "*this green paper illustrates the power of applying cooperative, multi-stakeholder principles*"!

We celebrate the process applied by the DoC IPTF and the results achieved thus far. We consider this to be a clear indication of the US Government's commitment to leadership in pursuing international, truly inclusive and collaborative processes. We look forward to seeing the fruits of this critical endeavor, to find solutions that ensure commercial data privacy in a way that protects the legitimate interests and maintains the trust and confidence of all stakeholders.

2. Praise for statements found in the Document.

2.1 Praise

> *"The following report – or green paper – recommends consideration of a new framework for addressing online privacy issues in the United States. It recommends that the U.S. government articulate certain core privacy principles—in order to assure baseline consumer protections—and that, collectively, the government and stakeholders come together to address specific privacy issues as they arise." - page i*

We agree with the goal of assuring baseline consumer protections. We applaud the recommendation to bring together a collaborative process to address specific privacy issues as they arise.

2.2 Praise

> *"To this end, the green paper recommends reinvigorating the commitment to providing consumers with effective transparency into data practices, and outlines a process for translating transparency into consumer choices through a voluntary, multi-stakeholder process." - page ii*

---

[1] http://www.think-trust.eu/downloads/public-documents/riseptis-report/download.html

Agreed. Empowering the consumer (through transparency, choice and other mechanisms) is also a clear EU objective.

2.3 Praise

> *"**4. Ensure Nationally Consistent Security Breach Notification Rules.** Finally, we recommend the consideration of a Federal commercial data security breach notification (SBN) law that sets national standards, addresses how to reconcile inconsistent State laws, and authorizes enforcement by State authorities. " - page 7*

From the perspective of a micro business, a consumer, an information security advocate and an international software development house, uniform and consistent commercial data security breach notification within the U.S. (and elsewhere) appears highly desirable.

2.4 Praise

> *"Drawing on the Task Force's analysis of the current framework and informed by the insights of NOI commenters, our framework relies on five main recommendations. First, we recommend adoption of a comprehensive set of FIPPs to protect the privacy of personal information in commercial contexts not covered by an existing sectoral law. Second, we propose to use commitment to a comprehensive FIPPs baseline as the basis for recognizing expanding interoperability between U.S. and international commercial data privacy frameworks. Third, to maintain the flexibility of the current U.S. commercial data privacy policy framework, an integral part of our Framework is to allow adherence to voluntary industry codes of conduct. Fourth, we propose to create a new Privacy Policy Office within the Department of Commerce to help provide the Administration with greater expertise and a renewed focus on commercial data privacy. Finally, we recommend setting a national standard for notifications following security breaches involving personal information in the commercial context. "*

We fully agree with the five recommendations above.

2.5 Praise

> *Enhancing transparency, though critically important to improving privacy protections, may not be sufficient. Plain, accessible statements about information collection and use do not necessarily bring these practices into line with consumers' expectations. An entity that clearly states that it intends to do anything and everything with the data it collects may be transparent, but it may not be providing adequate protection for consumer privacy. - p 38*

We agree with the principle and spirit of this statement, in particular for social web services and e-commerce!

2.6 Praise

> *"A complementary approach would encourage companies to enhance transparency through privacy impact assessments (PIAs). As discussed by several commenters, PIAs require organizations to identify and evaluate privacy risks arising from the use of personal information in new technologies or information practices. PIAs could also bring about useful transparency.*
>
> *If prepared in sufficient detail and made public, PIAs could create consumer awareness of privacy risks in a new technological context, where norms are not yet clear. PIAs could also help organizations to decide whether it is appropriate to engage in the particular activity at all, and to identify alternative approaches that would help to reduce relevant privacy risks. "*

…

> *"the value of transparency, purpose specification, and use limitations ultimately depends on how well organizations follow the practices to which they are bound. Auditing and accountability play a critical role. Audits compare actual data use against specified uses, and accountability is the capacity of an organization, or an enforcement authority, to discipline deviations from specified information uses or privacy policies. A means of verifying—to people within an organization and to*

those outside—that an organization has observed its stated limits on data use is essential to building and maintaining consumer trust." - p40

After having reviewed the use of privacy impact assessments in the NISTIR 7628 publications[2], and how this has helped shape their evolving recommendations, we strongly agree with the systematic use and publication of PIAs. Furthermore, we feel it would be excellent if 'easy to understand' PIAs were made routinely available to the user, at the point of decision, with regard to performing an electronic action.

PIA's may also work to inform organisations decision making processes when considering the adoption of new technologies. To quote Melissa Hathaway[3], speaking at her keynote presentation at the ORNL CSIIRW-6 in 2010:

"I Don't trust hardly any transaction right now, there is no integrity in our infrastructure. I don't care if it's available, you need to make sure it's a trusted transaction first, confidential second, and available third. And I think there are a lot of leaders in our country and around the world that would agree with me.

As we race to embrace, buy and integrate the next generation of technology into our lives and our businesses, do we really understand the vulnerabilities and exposure points and subsequent risks that are bundled with that purchase?

And I guarantee you the answer is no from a corporate environment.

And I can pretty much guarantee you that it is a no from a Government environment.

So that is a pretty good risk we just accepted, because we don't understand the technology, we don't understand where it is operating within the seams of this band-aid approach with this band-aid approach, with this operating system, and this new widget that gets introduced.

The attackers are exploiting those seams against us. How do we start to think about that?"

3. Constructive feedback on statements found in the Document

3.1 Feedback

To promote informed consent without imposing undue burdens on commerce and on commercial actors, FIPPs should promote increased transparency through simple notices, clearly articulated purposes for data collection, commitments to limit data uses to fulfill these purposes, and expanded use of robust audit systems to bolster accountability. - pg 4

We could not agree more strongly. Within the U.S. accessibility to privacy should not discriminate against the young, the cognitive impaired, or the busy. With regard to *international* customers of U.S. based Internet services many do not have English as a first language; a large number may have difficulty understanding English, or may even rely on automated translation services. Protection should not be limited to those who speak English with exceptional technical or legal language comprehension skills.

Yet, we urge caution. Simplicity should not be used as a way to "white wash" the devil in the fine print details. To protect against this there may be a need for organisations to err towards protecting the privacy of the customer, as

---

[2] The Smart Grid Interoperability Panel Cyber Security Working Group. NISTIR 7628 - Guidelines for Smart Grid Cyber Security. Interagency Report 7628, National Institute of Standards and Technology, Sep. 2010.

[3] Melissa Hathaway was named the Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils on 9 February 2009, and placed in charge of a 60-day interagency review of the plan, programs, and activities underway throughout the government dedicated to cyber security.

opposed to pushing the limits of what might be considered appropriate in exploiting such information for commercial gain.

3.2 Feedback

> *"Encourage the development of voluntary, enforceable privacy codes of conduct in specific industries through the collaborative efforts of multi-stakeholder groups, the Federal Trade Commission, and a Privacy Policy Office within the Department of Commerce."*
>
> *"Foundational principles, such as enabling individuals to give (or withhold) informed consent before information about them is collected, used, or disclosed in a commercial context, must guide efforts to strengthen commercial data privacy. At the same time, commercial data privacy must be protected in a way that does not stifle innovation or disregard the potential value, to consumers and companies alike, of appropriate data-sharing. Finally, the global dimension of commercial data privacy policy requires close attention, not only to enable the flow of commerce, but also to prevent conflicting policy regimes from serving as trade barriers." - pg 20*

We applaud this overall approach as an excellent first step.

However, we observe that the above text does **NOT cover a complete data life-cycle approach** to user-centric data privacy and data control. The user/business does not maintain contact/control with their sensitive data through it's life-cycle of creation, duplication, distribution, and (one would hope in many cases) ultimate destruction of the sensitive data.

Our observation is that once personal information has been exposed and traded to one or more additional third parties, there are currently **no practical** methods whereby consumers can uniformly track or control that information real-time. It is currently not possible to **comprehensively** take that personal information out of circulation, not least because I do not know with confidence who has it, and there is no efficient way for me to enforce it.

For example, I provide my information to a software-as-a-service provider, who then passes the information on to 3 other software-as-a-service-providers. I am not informed of the subsequent re-distribution to organisations that I do not have a direct relationship with. If there are some *N* organisations, what assurances do I have, and how can I determine if the *N* organisations will respect the usage terms that was presented to me by the original software-as-a-service provider?

For this reason, we feel it is critical that there be a minimum set of accepted standards, **with regard to the ability for an entity to track and control their sensitive information entrusted to others**, which must be applied by all organisations.

> *"Finally, the global dimension of commercial data privacy policy requires close attention, not only to enable the flow of commerce, but also to prevent conflicting policy regimes from serving as trade barriers." - pg 20*

Also, the list of issues noted after *"the global dimension of commercial data privacy policy requires close attention"* should be expanded to include "to ensure that privacy standards in one jurisdiction are not compromised in another".

3.3 Feedback and proposal

Moving toward the goals of enhanced transparency, as set forth above, however, may require an approach that goes beyond providing users with more direction toward privacy policies ***and means to manage their profiles****. -p 34*

We propose the following straw-man elementary rules:

1) Notification of receiving information to the customer;

2) Notification of what they are using it for;

3) Notification on each occasion they forward the information to a third party (triggering corresponding notification to the consumer by the receiving organisation);

4) Providing an avenue for customers to centrally track this movement; and

5) The ability to selectively revoke access to that information;

6) A process of redress for non-compliance with destruction requests.

In such case, the stakeholder is "in control of their personal information", and the burden is placed on organisations receiving data to register their possession and use with the individual.

If a customer incorrectly comprehended the impact of a privacy policy they agreed to, they can make amends after the event. e.g. issue a command to revoke access to my personal data from any organisation that received it directly or indirectly from this source.

Furthermore, **this would provide a basic audit mechanism whereby customers can determine if their expectations with regard to privacy are being met.** [e.g. if one company acts inappropriately by handing data to another honest organisation without permission, and that honest organisation receiving the data flags reception to the user, then there is a system of checks-and-balances in place to protect the user.]

I am not aware of any such an automated system currently in existence.

Such a user-centric system would appear to be in line with high-level objectives published within the U.S. and E.U.

4 Comments on the DHS FIPP on p 26

We make the following comments regarding the DHS fair information practice principles. These comments should be considered in all fair information practice principles.

4.1 FIPP: Transparency

"Transparency: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information"

We would like to see this extended to specifically include advertising bodies. For instance, if I use Facebook, or Google, and an advertising company receives personal information about me (including my personal preferences or behaviors), I should be informed at that time what information was provided, on what conditions they received it, will they sell that data on, and who I can contact if I want to remove this data about me.

4.2 FIPP: Individual participation

Individual Participation: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.

Based on personal experience, in practice, this process appears to occur only once: at the point where my information is disclosed by me. There is no enforcement of participation through the life-cycle of data usage. E.g. while I may have to authenticate myself to the organisation when I wish to perform a transaction (such as checking an account balance), there is no reciprocal process of transaction authorization on data already collected. E.g. Event Notice: do you explicitly permit us to {sell, or pass on for some other reason}, your information to this named organisation? If the answer is yes, then consequently, the recipient organisation should be responsible to notify you of that receipt, and then keep you informed during the entire data life cycle.

4.3 FIPP: Individual participation

> *"Purpose Specification: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used."*

In addition it would be desirable to have "data-flow specification". What systems will my data be received by? What is the purpose of those systems? What named organisations will you pass it on to?

4.4 FIPP: Data Minimization

> *Data Minimization: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).*

Organisations should only collect data that is lawfully allowed, directly relevant and necessary.

Pertinent questions may include, "Is the stated purpose directly or indirectly in the legitimate interest of the stakeholder?"

Sometimes the collection of data, "for the stakeholder's benefit", is highly suspect. Consider the hypothetical use statement: "*We collect all your personal contacts so we can use that information to help you promote our product to your friends.*" Such a use-case, with dubious value to the client, should require explicit consent for that purpose. Most importantly, access to a free / low-cost service should not be conditional on the user consenting to exposing their social contact details to support the company's marketing strategy.

4.5 FIPP: The need for "principle of least privilege" to be mandatory as a base-line data privacy requirement

> *• Security: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.*

The above listed security properties are not sufficient, we require also the principle of least privilege to be applied.

To quote wikipedia, the principle of least privilege requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user or a program on the basis of the layer we are considering) must be able to access only such information and resources **that are necessary for its legitimate purpose.**

Additionally we must ensure only those actors that "need to know" are exposed to the inputs or the results of a transformation. The term "need to know", when used by government and other organizations (particularly those related to the military or espionage), describes the restriction of data which is considered very sensitive. Under need-to-know restrictions, even if one has all the necessary official approvals (such as a security clearance) to access certain information, one would not be given access to such information, or read into a clandestine operation, unless one has a specific need to know; that is, access to the information must be necessary for the conduct of one's official duties.

e.g. It is not clear that Facebook is selectively forwarding client information, on a field by field basis, to 3rd party applications on a Need to Know basis after assessing the nature of the service being offered by that application.

4.6 FIPP: User Control

It would seem prudent to have a commercial data privacy policy that empowers users with the ability to efficiently manage and delete their personal information. E.g. Facebook does not currently provide an easy manual or periodic way to delete information after some *X* number of days. It is unreasonable to expect a user to have to manually delete a year's worth of old information manually (potentially thousands of discrete delete steps). **Our concern is, that where customer data is seen as value to a company, that company has no incentive to reduce it's asset base by making it easy for customer to improve their privacy through selective destruction.**

4.7 FIPP: Accountability and Auditing

> *• Accountability and Auditing: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.*

Consider mechanisms that permit the client to see the internal company audit logs that relate to access of their personal data. How often was it accessed, by who (at least by an identifier that can be resolved internally by that company) and so on.

4.8 FIPP: Data de-personalisation

We feel that data de-anonymizing techniques for commercial exploitation should be considered for prohibition. It does not appear appropriate (to us) for a commercial organisation receiving anonymized data to then correlate that information with other data sources to identify individuals, and to use that resulting information against the individual (such as for financial gain). **This goes against the spirit of the conditions on which they received anonymized / depersonalized data.**

To be clear, I am not saying researchers should not continue their studies enquiring as to the effectiveness of aggregation and anonymizing techniques. This is important research that should be funded for the benefit of the community at large. See the following 2 researchers for more information on data de-personalization:

http://33bits.org/2009/03/19/de-anonymizing-social-networks/ and www.jeffjonas.typepad.com

5. Constructive feedback to questions asked

Please find our responses to the following selected questions sourced from "Federal Register/Vol. 75, No. 244/ Tuesday, December 21, 2010/Notices".

5.1 Exploring safe harbors against FTC enforcement for practices defined by baseline data privacy or voluntary, enforceable codes.

> *"Businesses generally recognize that their sustainability depends on maintaining consumer trust but find that the rules of the road are hard to discern, and sometimes become clear only after FTC enforcement actions." - p22*

It would appear to us, that organizations that have a large customer database, or rather manage personal information on a very large number of entities, have a greater burden of responsibility to maintain. With regard to establishing a safe harbor for organisations that manage greater than *X* (lets say 500,000 for purpose of this discussion) persons, that those high-risk organisations should be encouraged to employ a pro-active government-public consultation approach that seeks to address privacy concerns before they implement them. In this way, for organisations that could expose v. large numbers of people, their proposed privacy policies could be vetted, and applied, with the provision of providing a penalty-free path to revise and amend them in response to FTC enforcement or community value changes (on the proviso that the organisation is behaving in good faith).

5.2 What is the best way of promoting transparency so as to promote informed choices? The Task Force is especially interested in comments that address the benefits and drawbacks of legislative, regulatory, and voluntary private sector approaches to promoting transparency.

Observation 1

As described in section 3.3, we would like to see transparency implemented in such a way that the customer, at any time, maintains situational awareness / understanding of their sensitive data assets that are residing in 3rd party systems.

"*Situation awareness involves being aware of what is happening around you to understand how information, events, and your own actions will impact your goals and objectives, both now and in the near future.*"[4]

"*Situational understanding* ***is information scaled to one's level and areas of interest****. It comprehends one's role, environment, the adversary, mission, resource status, what is permissible to view, and which authorities are relevant.*" … "*Situational understanding includes the state of one's own system from a defensive posture irrespective of whether an attack is taking place.*"[5] -

This concept of transparency should be extended to include awareness of risks and threats. It should require organisations to inform their clients about the risks and require them to forward copies of warnings issued by relevant authorities and experts.
See also: http://www.whitehouse.gov/blog/2011/01/27/sharing-responsibility-our-collective-security

Observation 2

In this observation, we feel the current green paper text does not go far enough in highlighting the competing interests of commercial advantage, the financial value of data exploitation, and the competing impacts of applying clear and adequate privacy protection practices. Specifically we observe that:

" Transparency and appropriate privacy practices must be squarely aligned with commercial success. The opposite must be squarely aligned with commercial failure in the market place. "

Currently, a lack-of-transparency wrt. to privacy practices MAY result in commercial advantage to some companies that should not, or would not have, been granted access to certain personal information. A lack of transparency may enable a company the ability to exploit information that a customer might choose otherwise not to disclose.

From a cyber-economics perspective, we must ensure that crime / nefarious behavior does not pay.

To set the monetary value of personal information in context, Goldman Sachs currently values Facebook (2011), a social media company entrusted to manage personal information of more than 500 million active users, at a $50 billion valuation, that is $100 for every active user. This aggregated information is selectively passed-on to Facebook application providers. On the other end of the spectrum, criminal organisations that have acquired personal information through nefarious means sell that information on the black market.

To promote the adoption of transparency so as to promote informed choices, a system of checks-and-balances must be arranged such that a company that chooses not-to-be transparent, or chooses to employ inappropriate privacy practices, cannot be commercially successful, and those that achieve the highest level of transparency and privacy protection are rewarded, as are those that move towards goodness. It is critical that the rewards for

---

[4] http://en.wikipedia.org/wiki/Situation_awareness

[5] https://www.fbo.gov/utils/view?id=bea326bcd2453cc43f8d4c2beb150964

transparency and privacy preservation, and the subsequent loss of commercially exploitable information, out weighs the fiscal returns from exploiting information gleaned through a lack of transparency.

Observation 3

In this observation, like the former, we focus not so much on a particular 'approach' to promote transparency, but rather on what we observe might be present in a successful approach. In this case, instead of appealing to financial returns as in the former, a concerted and well thought out call to virtue and the protection of the legitimate interests of the community might be made.

To quote the Spirit of Laws (1748), book 5, chapter 18 "Of rewards conferred by a Sovereign":

> *"… in a republic where virtue reigns — a motive self-sufficient, and which excludes all others — the recompenses of the state consist only of public attestations of this virtue. It is a general rule that great rewards in monarchies and republics are a sign of their decline; because they are a proof of their principles being corrupted, and that the idea of honour has no longer the same force in a monarchy, nor the title of citizen the same weight in a republic."*

In part, we can see the "voluntary" process already underway as a public call for virtuous behaviors to be defined by the community, for the community. The green paper has already identified how many commercial organisations already recognize the importance of good-standing in the community, that protecting the stakeholder is in their own interests.

Maybe this spirit could be enhanced somehow.

It would be desirable, that when momentary outcries regarding burdens are made, these complaints could be systematically and thoughtfully met with praises of that organisations' virtue by taking on that burden, and recalling the subsequent benefits to the community as a whole. "We do this, because it is the right thing to do. If you want to know the details of 'why the community believes it is the right thing to do', read more here [insert link]".

Likewise the issuance of honorary titles to organisations with leading privacy practices (on the ground) could also result in preferential government treatment (contracts) and community status. E.g. encourage media to note when a company is or is not a privacy leader in it's media notices.

Observation 4

The role of educating the community as to "current practices", for the purpose of raising awareness of their personal risks and threats, enabling the community to make better informed choices, is important. For example, the systematic documentation of the current market practices through media such as the television can help people become aware of what is actually being done, and what is at stake. This could be enhanced by funding additional research into evaluating the actual impacts of loss of data privacy within the community, and feeding those results back into documentaries that are aired on public broadcast stations / discovery channel.

However, it is somewhat disadvantageous to the stakeholder to require "honorable" organisations to list all the myriad of things they "don't do", where as "less honorable" companies need not make statements about those same items which they exploit for financial gain. The assumption that organisations are expected to be less than virtuous by *de facto* undermines the communities expectations of the way commercial organisations should be behaving.

In addition to an organisation having to state WHAT they do, I would appreciate them outlining some of the significances of a choice. e.g. "*We sell your personal data, and personal behaviors, for a profit, and that data then*

may be resold again for a profit. We don't tell you who we sell it to, neither do they, and you cannot easily recover your privacy after it has been sold. The Internet does not know how to forget[6]*. "*

5.3 What incentives could be provided to encourage the development and adoption of practical mechanisms to protect consumer privacy, such as PIAs, to bring about clearer descriptions of an organization's data collection, use, and disclosure practices?

Suggestion 1:

> *In particular, one commenter identified potential class action liability as one of the "largest hurdles" that companies face when they seek insurance and contract with other entities that handle personal data.*

Might it be possible to create a standard pro-forma template, with regard to checking due-process expectations with regard to applying PIA's and other forms of best security practices, that helps insurance companies identify those organisations that are less likely to face class action liability? Maybe they already have such a template.

Suggestion 2:

With regard to accelerating the adoption of a comprehensive set of FIPPs to protect the privacy of personal information in commercial contexts not covered by an existing sectoral law, we offer the following thought.

To provide greater commercial incentive to meet the community's social expectations, the early adopters (who pass independent audits) could be rewarded by a % of the penalties applied and collected against those who do not achieve compliance within a generous but fixed time-frame. If set up correctly, it may be possible to make it commercially competitive to be openly transparent, as lagging organisations are paying for your compliance efforts. Conversely, in the ideal case, all organisations achieve compliance in time, in which case there is no redistribution of wealth. This could be applied to the top *X* thousand corporations with the largest data-sets.

A similar principle of penalizing foreseeable security breaches (loss of control over personal information) and redistributing the penalty proceeds to organisations that can demonstrate they are actively investing in adequate security controls (personnel + technology) could provide a commercial advantage to those organisations in the community. The goal being to have a self-financing rewards and penalty mechanism that encourages transition towards socially acceptable practices. In effect, because of the foreseeable and preventable breach, the offending corporation ends up giving money to their competitors. This makes a more pointed and effective message than when penalties are just being paid to the Government. The process should include in its scope the potential for one organisation to attack a competitor (causing a data security breach) and ensuring that the risk of getting caught outweighs the potential financial returns through the subsequent penalty redistribution. Penalties should be independent of claims for damages.

5.4 What are the elements of a meaningful PIA in the commercial context? Who should define these elements?

We would look to NIST to co-ordinate this work with input from the public and private sectors. It is possible that NIST may already have something similar to this covered in their SP 800-xxx series that they might be readily able to adapt. If they don't, then maybe they would find it is useful to write a guidance document on writing PIA in the context of both commercial and Government systems. Advantageously, NIST could then also extensively cross reference other NIST special publications to help commercial organisations employ good security practices that are already documented but organisations may not be aware of.

---

[6] http://online.wsj.com/article/SB10001424052748703555804576101591825228076.html

5.5 Should there be a requirement to publish PIAs in a standardized and/or machine-readable format?

We feel this should be explored. One way might be to create a basic template for well identified risks, and controls used to mitigate those risks, and then support 'expansion' in human readable form to outline additional details. This would then help tie into the use of NIST SP 800-53 which lists security requirements and controls in a standard way. The machine readable format would probably support limited automated analysis, and quickly enable the system to present to users any non-standard risks.

5.6 What are consumers' and companies' experiences with systems that display information about companies' privacy practices in contexts other than privacy policies?

Personally speaking, I have only met with two pure Internet services, over the last 12 months, that have presented me with informed disclosure on how my personal information might be used to complete a transaction. I have found this information helpful in prompting me to make a conscious choice to perform or not perform an action. It happened that, in both cases, I chose not to proceed as I considered the disclosure onerous and not directly relevant to the transaction I wished to perform. [To be clear, it was not because I was asked, but because I felt the information they requested was inappropriate/not necessary to the transaction I wished to perform].

Unfortunately, in both cases, the choice was "disclose the full information I request" or "do not proceed with the transaction". I did not have the opportunity to only disclose the information that I felt was appropriate to the purpose. I felt that there was an element of **coercion** being applied against me whereby I wanted to perform the transaction but this was denied unless I consented to what I considered to be an inappropriate level of disclosure. I feel that if it became common practice to disclose how information would be used, organisations that asked the appropriate level of information would be more successful than those seeking unrelated information especially when organisations seek inappropriate data in a seemingly coercive manner.

The collection of data and seeking consent for the collection or further use of data beyond the required minimum should not be permissible as a condition of obtaining a good or service, as this would be a violation of the least privilege principle.

When appropriate standards of data collection are in place, then privacy experts (and other experts) can more easily rate and inform the public on organisations comparative performance. This opens the whole problem of data having potential (often undisclosed) commercial value to the gatherer, whereas it is personal and private to the provider.

Let us now consider my experience with Facebook. To use a Facebook application I must permit them complete access to my social network of connections and personal interests, even though this information is not related or required in the delivery of the particular service I wish to receive from that application. e.g. A friend, using a Facebook application, sent me a (presumably) cute picture as a gift through the Facebook platform. I receive a notification saying that the application provider will only let me see this gift if I register with it and completely expose all my social connections to it. Clearly, this is personal information about me that the application does not require to be able to fulfill the discrete function of sending me this image/gift. Thus, we have a violation of the least privilege principle. To complicate matters, by rejecting my friends gift, I am sending a message to my friend that I do NOT want to send (I reject your thoughtfulness). In short, I am given the choice of rejecting my friend, or supplying my personal data to an unknown, and untrusted application provider. This comes across as seemingly coercive.

Facebook does not permit me to control what information I disclose in a granular nature, **and the Facebook application provider has no commercial interest in reducing the amount of information they demand.**

Likewise, asking for information which provides me with an 'enhanced' service to promote that application to my friends, or to use information about my friends to promote their service as valuable, should be optional and made

available only on my request. Furthermore, that information should be limited in use to that transaction, and not permanently stored.

In all cases, there was no easy way for me to directly communicate what my expectations were, or how they might remedy the situation so that I would feel confident using their service.

Additionally, I am also concerned that when I unsubscribe a service, such as a 3rd party Facebook Application, that the principle of data minimization will not be applied, and my personal data which is no longer required to perform any function, is not destroyed.

5.7 Are purpose specifications a necessary or important method for protecting commercial privacy?

Yes. In fact, I would go one step further and propose that data-flow specifications of the system, outlining all consumers and producers of information used in that system, should be outlined and maintained by larger organisations.

5.8 What incentives could be provided to encourage companies to state clear, specific purposes for using personal information?

Consider aggregating a large collection of statements detailing clear and specific purposes for using personal information in a freely online, public domain, database. This serves two purposes: 1) It advertises those organisations that present particularly clear information, 2) It enables many others to find the closest clear statement that matches their operations that they could then adapt. This creates a rewarding community that empowers other organizations to adopt clear statements. You could consider a competition, which is more about status than money, that rewards innovative or excellent new submissions -- or preferably best total-service disclosure statements. e.g. Company X has one of the most transparent, easy to understand, purpose statement covering the services provided. Such companies should be audited before rewards are publicly announced to ensure the statement matches the apparent reality on the ground. Rewards, or at least supportive announcements, should be made by any organisation that had to make a particularly large effort (given the complexity of the business process).

5.9 Who should be responsible for demonstrating that a private sector organization's data use is consistent with its obligations?

This is an extremely hard question. We feel internal audits are necessary, and external audits may also be necessary. Unfortunately, it is not clear to us that internal audits will be sufficient to engender adequate levels of trust, and we are concerned about the expense of adequate levels of external audit - most particularly for small to medium sized enterprises / startups.

Audits should be designed in such a way that they do not prevent innovation or the development of products. Or rather, development processes should be adapted so audits regarding data privacy can be readily achieved.

To perform an audit, there is a need to be able to review specifications at a high level, and dive down into the source code where required. This is extremely difficult in some systems which do not currently have a well-documented specification. Would auditing result in some types of (arguably poor) development practice being banned? Would small businesses be prevented from entering the market due to the additional paper work or insufficiently high development standards? Conversely, if we did not audit small businesses, would this then become the deployment vehicle of choice for deliberate and systematic abuse of privacy?

Should we simply insist that ONLY organisations that are subject to external audit and that apply adequate internal audits MAY distribute private data AFTER obtaining the persons consent on each such event? To put that another way, organisations without those audit checks should NOT be allowed to even request consent from people, because there is no way of ensuring compliance. A certification process could be developed whereby organisations could become 'certified' as having the right audit and other mechanisms in place necessary to win the authorization

to seek consent. This provides the incentive to adopt the best practices and to become certified, while not mandating audits upon all organisations.

Our concern with internal audits, is that self-regulation works best in those organisations that have an inherent desire to act with integrity wrt. to that regulation. That is, where the regulation is perceived to be aligned with the stated and actual goals of the organisation. This may be self-evident, but we include our thinking for completeness in our reply. By way of illustration of the positive, many manufacturers of high-assurance equipment can be reasonably expected to apply due-diligence in applying self-audits as described in the IEC-61508 standard. This is because the direction of the company (to create high assurance products), and the customers expectations (we really need this to work), are fundamentally aligned with the self-audit (to validate we have achieved high assurance products). However, if a company has over committed itself, or finds itself in tight financial situation, it may find it expedient NOT to apply the necessary rigor in applying self-audits to achieve the necessary level of assurance. The commercial pressures to "get the system online and sell something" is always extremely high. Failure to do so in adequate time can result in commercial failure.

5.10 Are technologies available to allow consumers to verify that their personal information is used in ways that are consistent with their expectations?

Not that I am aware of.

A well known part of the problem is that once information is exposed in human readable form, or can be stored on removable media, all ongoing control mechanisms are lost.

It follows that controls must be in place to prevent the large-scale clear-text exposure of sensitive data. e.g. a database of user names and details might be extracted and sold on a one-time-basis by a privileged user, even though the 'audited system' has no such mechanism and might itself comply with all privacy statements. This implies the entire information system must be designed in such a way that privileged staff (managerial, technical, customer support) acting unilaterally cannot override or subvert the security controls, even during debugging, upgrade and transitioning to another system. Furthermore, such a system should not permit those provisioning the software (operating systems, firmware, …) or hardware (chip manufacture, product manufacture, …) to remotely compromise the system.

Unfortunately we are not aware of any commercially available solutions that can achieve this base-line result today.

Synaptic Labs is in the process of designing and implementing a computing platform and operational process that is designed to comprehensively address the issue of processing sensitive data in a way that comprehensively protects it from a very broad range of both insider and outsider attacks. Visit this link for more information:

http://www.ictgozomalta.eu/vision-and-projects/project-tc2p.html

5.11 What incentives could be provided to encourage companies to adopt technologies that would facilitate audits of information use against the company's stated purposes and use limitations?

See the comments about CERTIFICATION above.

Maybe the community might try to find ways in which specific technologies can make a clear business case showing how increased PROFITS can be made shortly after deployment (pays for itself), and not how potential but not-yet realized LOSSES can be mitigated.

If possible, try to encourage technology developers to integrate the functionality as an integrated and indivisible part of their next generation offerings. In this way, organisations seeking the commercial benefits of improved technologies have ready access, and are encouraged to use the features that help the company achieve it's stated purposes and use limitations. Of course, technology developers would prefer to be able to make a significant profit from offering new features that met requirements that are mandated on the customer by a higher power.

Mandating a requirement may make it more expensive on the client, but in many cases they may simply not choose to adopt a risk-prevention functionality otherwise. This can be a justifiable approach particularly in such cases where the potential for negative impact goes beyond a loss that only affects the client themselves. Certain personal information is important across a vast array of identity systems and applications, and more needs to be done to help end users become more aware of the interdependencies and potential consequences. Thus informed clients may be more willing to pay for enhanced functionality in products and services.

It might be argued in many cases, the local community, regional community, the nation and society as a whole is not adequately considered in high-level corporate decisions. Furthermore, certain short-term commercial advantages are gained by those that do not apply such measures. Through appropriate standards, public education and levels of certification of organisations, end users may select between providers based upon their level of certification, allowing organisations that make responsible, but initially costly, risk management decisions to win a competitive advantage (we offer you better levels of security assurance) and allowing the option to charge more for that level of service. Unfortunately, charging customers for a better base-line security, may place at risk lower-income brackets. Additionally, customers may not appreciate the true-value of the additional security measured offered, or have the training to assess the actual level of risk they are exposed to, so as to select the most appropriate option.

See the following document for one example of research exploring approaches for fairly distributing the costs to install/maintain a given level of security functionality that protects the legitimate interests of all stakeholders in shared information processing systems:

Aissa, A., Abercrombie, R., Sheldon, F., and Mili, "A. Quantifying security threats and their potential impacts: a case study". Innovations in Systems and Software Engineering 6 (2010), 1–13. 10.1007/s11334-010-0123-2.

5.12 Should a preemption provision of national FIPPs-based commercial data privacy policy be narrowly tailored to apply to specific practices or subject matter, leaving states free to regulate emerging technologies? Or should national policy, in the case of legislation, contain a broad preemption provision?

> *Some commenters argued that national consistency in commercial information privacy protections would make compliance simpler for businesses, and could help consumers better understand what privacy protections cover their information on the Internet. --- In contrast, other commenters disfavored preemption, arguing that State legislatures are in a better position to create regulations, both because State legislatures are better able to respond to consumer concerns, and because State legislatures are better able to create innovative approaches to regulation of quickly developing technologies.*

As a small business, we would prefer to be able to focus on just one set of laws and know we have uniform compliance across all states. However, we would like to feel that the laws were responsive to technical and social changes.

We note that the green-paper states:

> *Thus, the Dynamic Privacy Framework can help accelerate the current iterative process (reform of privacy practices following complaints from individuals and privacy watchdog groups, FTC investigations, and Congressional hearings). - p 69*

Maybe the Dynamic Privacy Framework could be enhanced somehow to co-ordinate the activities at the state and national legislatures. To provide a straw-man example, enabling innovation to take place at the state level, with regard to *identifying* proposed regulatory changes, and drawing together state legislatures and federal legislatures to periodically refine the broad baseline National laws based on their collective evolving experiences.

5.13 The Task Force seeks case studies and statistics that provide evidence of concern—or comments explaining why concerns are unwarranted—about cloud computing data privacy and security in the commercial context. We also seek data that links any such concerns to decisions to adopt, or refrain from adopting, cloud computing services.

We submit the following publications, with those marked with an asterix as must pertinent:

** Catteddu, D. Security & Resilience in Governmental Clouds – Making an informed decision. Report, European Network and Information Security Agency, Jan. 2011.*

** Privacy Committee, W. C. C. S. Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies. paper., U.S. CIO Council, Aug. 2010. http://www.cio.gov/Documents/Privacy-Recommendations-Cloud-Computing-8-19-2010.docx*

** Dietz, R. Maintaining Control and Compliance in Cloud Computing: Data-centric Information Security. Webinar BrightTalk Webcast 6942, SafeNet, Mar. 2010.*

Catteddu, D., and Hogben, G. Cloud Computing - Benefits, risks and recommendations for Information security. Report, European Network and Information Security Agency, Nov. 2009.

Jaeger, P. T., Lin, J., Grimes, J. M., and Simmons, S. N. Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing. In first monday (May 2009), vol. 14. http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2456/2171

Our organisation refuses to store our commercially sensitive data as cleartext in public clouds, in any country. Our primary concern is that privileged technical and managerial staff of public cloud providers who have access to commercially valuable information from tens of thousands of businesses may access our private data for personal gain. This concern is not unfounded, see:

> *Krazit, T. Google fired engineer for privacy breach. News article, news.cnet.com, Sep. 2010. http://news.cnet.com/8301-30684_3-20016451-265.html*

Our secondary concern is that third party service providers are being forced by various regional laws to act as data collection, retention, and distribution agents for various Governments. This concern echos those concerns expressed within the EU and the US in the first two links mentioned above. We perceive, in general, the line between law-enforcement activities and intelligence gathering to advance various (open-ended) national interests has become blurred; maybe it has always been. See also:

> *Tim Greene, Former NSA tech chief: I don't trust the cloud, ComputerWorld, 2010. http://news.idg.no/cw/art.cfm?id=2A175B19-1A64-6A71-CE0091748622030A*

Our concern is any technology that empowers law enforcement agencies, will simultaneously support international commercial espionage by other agencies within that same government. Furthermore, backdoors inserted by a 'legitimate' agency can be exploited by others.

See Bruce Schneiers expose on the GMail issue in China:

Schneier, B. "U.S. Enables chinese hacking of Google". In CNN Opinion (Jan. 2010), CNN. http://edition.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html.

See also the "Concerns of Nation States" section on the wikipedia page on "Industrial Espionage". http://en.wikipedia.org/wiki/Industrial_espionage#Concerns_of_Nation_States

Of course the risk of insider attacks goes far beyond trusted management, admin and technical staff. See also the risks of insider attacks hidden in the hardware and operating systems of devices deployed inside legitimate organisations (such as clouds) without their knowledge or consent. These types of insider and outsider attacks are problems identified in various agency calls for new IT security solutions and are specifically addressed in Synaptic Laboratories Limited new trustworthy cloud computing platform (TC2P).
http://www.ictgozomalta.eu/vision-and-projects/project-tc2p.html

6. Feedback on text

6.1 Proposed expansion on the text:

"Privacy protections are crucial to maintaining the consumer trust that nurtures the Internet's growth. Our laws and policies, backed by strong enforcement, provide effective commercial data privacy protections. The companies that run the digital economy have also shown a willingness to develop and abide by their own best practices. As we entrust more personal information to third parties, however, we can strengthen both parts of this framework." - pg iii

The companies that run the digital economy have also shown a willingness to develop and abide by their own best practices. As we entrust more personal information to third parties**, and as the number and diversity of third parties increases, we can and should** strengthen both parts of this framework.

6.2 Minor modification to the text:

"The United States is in a strong position to demonstrate that our framework provides strong privacy protections, and that the recommendations in the green paper will further strengthen these protections. " - pg iii

"The United States is in a strong position to demonstrate that our framework **also** provides strong privacy protections,"

6.3 Minor modification to the text:

"This engagement will provide the opportunity to reduce friction in the flow of personal information across national borders, reducing costs for companies and encouraging U.S. exports." - pg vii

"This engagement will provide the opportunity to reduce friction in the **appropriate** flow of personal information across national borders, reducing costs for companies and encouraging U.S. exports."

7. Requests / suggestions

7.1 Small business support

We have identified that small businesses, trading internationally, might be served by the establishment of a very conservative privacy policy standard that will provide them international safe-harbour. The trade-off from such a conservative policy may be that 'less information' might be collected by that company than what they might be permitted in some cases. The trade-off for the company being that the barrier to entry, and risk of compliance failure, should be dramatically reduced.

7.2 Establishing a baseline expectation

We feel it would be desirable, after performing adequate preparations appropriate to the task, to encourage every University to assign a project to the appropriately qualified students to perform extensive surveys establishing baseline expectations of privacy in the various segments of the community. A common pro-forma for collecting data, while leaving the questions actually asked open, may permit the process to collect a very wide range of opinions, on a wide range of questions, to identify what the expectations of the community are with regard to socially acceptable behavior regarding personal information.

Our intuition is that what is deemed reasonable privacy expectations to a technically educated person that understands the operation and limitations of conventional technologies as they are today is probably not what is considered reasonable by a lay-person who wishes to use technology to perform some task.

E.g. As a telecommunications expert, I understand why the 24/7 movement of mobile phones are inherently trackable by base stations, and even why it is possible in many cases to track people down to a few meters accuracy.

In the community, we see large numbers of people complaining about RFID being used to track people, but these same people not realizing that their mobile phone already track them and can be used by law-enforcement agencies (and therefore potentially others) for that purpose.

I understand that when technical specifications advertise that mobile phone use encryption, that this is protection is only applied between the phone and the base-station. I have talked to random people on the street who have told me that they thought their mobile phone call was encrypted, and did not realize that in fact it did not provide end-to-end security as they envisioned. They simply did not perceive of any other type of security mechanism.

We feel it is highly inappropriate to use 'expert technical knowledge' as the baseline for setting privacy expectations.

END