

ServasOnLine Senior Panel Teleconference

July 26, 2011

Attendees: Derek Carver (New Zealand), Penny Pattison (Canada), Phyllis Chinn (USA), Michael Silbert (Canada), Rodolfo Alvarado (Mexico), Gary Sealey (Canada), John Gunther (USA), Maritndrieu (France), Jonny Saganger (Sweden), Thomas Thomas (Germany), Pramod Kumar (India), Anna Cristina Siragusa (Italy).

Regrets: Ken Sturt (Britain), Pablo Colangelo (Argentina) – could not connect by Skype.

Chair: Gary Sealey

Draft Meeting Agenda:

- 1) Re-Introductions (all)
- 2) Status of Servas Online prototype (Pramod)
- 3) Read and reflect on Michael's proposal and the questions he addresses (Michael)
- 2) Understand the Privacy policies to which he points (Michael and all)
- 3) Consider what advice to give GA and national groups (Jonny)
- 4) Discuss decisions required to advance Servas Online (All)
- 5) other updates, schedule, networking and etc.
- 6) etc

Notes:

1. Re-Introductions and opening comments
 - a. Penny will send these draft notes to Jonny and Gary first for review, and then to the whole group.
 - b. Jonny is preparing ServasOnLine recommendations for the next GA. Some of these can be implemented as the project is developed further, before the GA.
 - c. The Terms of Reference for the ServasOnLine Senior Panel need to be updated.
2. Status of Servas Online prototype

Pramod gave an update about the Drupal prototype developed by Mathew Pashkovskiy (Russia)

 - It was initially set up on an Amazon server in the US, but moved to the Servas server recently
 - The link to it is drupal.servas.org
 - It is still draft, very new and untested
 - Four or Five participants logged into the prototype for the first time.
 - Everyone was encouraged to look at it to get an idea of the functions that are included in it now
 - Mathew will not be available until September 2011 to make any changes
 - Pramod will help people who have questions about the prototype
3. Read and reflect on Michael's proposal and the questions he addresses

Understand the Privacy policies to which he points

 - Michael gave a summary of the paper that he sent (see appendix A)

- He also explained about the different laws in different countries, and their history, and commented on the comparison between Canadian and EU rules (see Appendix B), as well as the USA and China privacy approaches
 - His draft recommendation is :
Moving forward with the development of ServasOnLine, Servas attempt to satisfy the policy requirements of the European Union, New Zealand and Canada privacy policies.
 - There was some discussion of how it is not possible to control all legal and security service issues in all countries; all that can be done is follow best practices related to our mission to redistribute host data to qualified Servas travellers
 - Some countries need to know the actual names of the people who manage the database and data
 - Several people expressed support for Michael's document
 - There was discussion of the need to differentiate sensitive from non-sensitive data, and it was emphasized that, like Couchsurfing, the Drupal prototype does not display sensitive data unless the host wants it shown
 - it was noted that movement of the data also needs to be treated carefully, e.g. compression and encryption when backing up the data to another server
 - The current model of paper or pdf host lists containing all data is a challenge; it was pointed out how insecure printed books are
 - Michael indicated that Servas Canada had recently implemented an electronic solution that provides reasonably safe access to pdfs; if others are interested they can contact him
 - The non-on-line Servas members also need to be considered, and therefore the ongoing need to convey sensitive host data to travellers in non-electronic ways
 - The crucial Servas paradox was mentioned: hosts want to be visited by Servas travellers, but they want their data to be safe and secure
 - It was noted that the Servas federated , decentralized governance model makes ServasOnLine more challenging to develop and implement
4. Consider what advice to give GA and national groups
- It is important to do a thorough analysis of the different regulations around the world to create policies and checkpoints to make the best possible secure system
 - Our main task is to create a system that serves Servas hosts and travellers , flexible and fast
 - Need to be thorough in examining the difficulties
 - Action: Michael Silbert will lead a group (including Jonny, Marite, Anna-Cristina, Thomas) to develop a draft **Servas International privacy policy for handing Servas data**; the plan is to distribute the draft for comments in late August 2011. Others are welcome to help as resource persons.
5. Discuss decisions required to advance Servas Online
- It was agreed that Use Cases are important, and needed to test the Drupal prototype, and to document what the system needs to do.
 - Action: Thomas Thomas is revising the Use Cases that were developed for the May 2010 Meeting. John Gunther will review Thomas' draft and add to it. The Use Cases will then be

circulated , at least a week before the Use Case meeting, to the whole group for thorough review and comment.

- Action: Gary will schedule a meeting of this group in about 3 weeks to discuss the Use Cases. Everyone agrees to review the documents before the meeting.

APPENDIX A: Servas Online Privacy Issues

The most valuable thing possessed by each Servas member group is the personal information of its members. This information, hereinafter referred to as personal content, has been entrusted to Servas by each member under the assumption that it will be secured against unauthorized access and use by the Servas member group to which the member belongs. It should be assumed that personal content held in trust by a national member group will be secured and the privacy of each member's personal content will be protected subject to all legal requirements established by that nation for the protection of personal privacy.

Different nations have established different requirements when it comes to protecting the privacy of personal content in electronic form. [At the time of writing, a crisis is unfolding in the United Kingdom concerning access to personal content in the form of unauthorized access to individual's cellular telephone calls by a news organization.]

A very brief survey of national legislation, around the globe, reveals vast differences in the way in which personal content is protected by nations. So what responsibility should Servas accept internationally --- and collectively --- for the protection of the personal content of members entrusted to it by member groups? And how does the fact that the privacy of personal content entrusted by members is limited by the fact that the reason for providing this personal content is in order that it be shared?

National member groups subject to privacy legislation that tends to be highly-developed and proscriptive will/should be hesitant to entrusting the personal content of their members to an environment in which the risk of loss of privacy is significantly greater due than that required by their own national legislation. As such, any international agreement regarding the security of personal content should strive to meet the most rigorous of the national standards. In the process, most --- if not all --- national groups can, with peace of mind, entrust their members' personal content for international use to such a secure environment.

Once personal content is disseminated, whether it be directly to hosts or through other national member groups, responsibility for ensuring that such content is handled in a secure manner and used only for the purposes for which it is provided is inherited by the receiver of the content. This is a matter of trust that has not been clearly reinforced in the past and that has, in some circumstances been ignored. This is something that goes to the heart of Servas, itself, since there is nothing more crucial to the existence of this organization than trust. In the event that this trust is broken in a significant or systemic way, the very existence of Servas could be in mortal danger.

If you wish to familiarize yourself with some of the more highly-developed privacy policies, I would suggest you consider the policies of the [European Union](#), [New Zealand](#) and [Canada](#). I recommend that, in moving forward with the development of Servas Online, that we attempt to satisfy the requirements of these three policies (at a minimum).

There are over thirty other "hospitality" organizations operating around the world, almost all of which

have sprung up in the last 10-15 years. To the best of my knowledge, virtually all of them are designed on single, centralized model for handling of personal content from its collection to its secure storage and controlled access. As a federation of national member groups, Servas is at a significant organizational disadvantage when it comes to delivering its services in the twenty-first century. Establishing a single, centralized platform for the delivery of our services is the easy part. Getting national member groups to cede some of their individual sovereignty for the overall good will likely be the hard part.

Respectfully submitted,
Michael Silbert

APPENDIX B: Comparison of Privacy – Canada and European Union

<i>Personal Information Protection and Electronic Documents Act (Canada -- 2000)</i>	<i>Data Protection Directive 95/46/EC (European Union -- 1995)</i>
	Notice—data subjects should be given notice when their data is being collected
Purpose—data subjects must be provided with the opportunity to know why an organization collects, uses or discloses their personal information Purpose—data subjects should expect an organization to collect, use or disclose their personal information reasonably and appropriately, and not use the information for any purpose other than that to which they have consented	Purpose—data should only be used for the purpose stated and not for any other purposes
Consent—data collectors must obtain consent when they collect, use or disclose their personal information	Consent—data should not be disclosed without the data subject’s consent
Security—data subjects should expect an organization to protect their personal information by taking appropriate security measures	Security—collected data should be kept secure from any potential abuses
	Disclosure—data subjects should be informed as to who is collecting their data
Access—data subjects should be able to obtain access to their personal information and ask for corrections if necessary	Access—data subjects should be allowed to access their data and make corrections to any inaccurate data
Accountability—data subjects should be able to complain about how an organization handles their personal information if they feel their privacy rights have not been respected	Accountability—data subjects should have a method available to them to hold data collectors accountable for following the above principles
Responsibility—data subjects should know who in the organization is responsible for protecting their personal information	
Accuracy—data subjects should expect the personal information an organization holds about them to be accurate, complete and up-to-date	
Non-withholdability— data-collecting organizations must supply an individual with a product or a service even if they refuse consent for the collection, use or disclosure of that individual's personal information unless that information is essential to the transaction	
Understandability—Organizations must have personal information policies that are clear, understandable and readily available	