LOI For Phase 2 Projects / Subprojects template

Completed Letters of Intent (LOIs) should be sent as email attachments to applications@grand-nce.ca with "GRAND Phase 2 LOI" as the subject line.

A successful proposal will address problems of significant relevance to the GRAND research program and must meet all of the guidelines for projects within GRAND, including the following mandatory requirements:

- The project must address significant research issues relevant to one or more of the GRAND Challenges identified for Phase 2 of the GRAND NCE
- The Project Leader and Co-leader must work at different universities; often they will represent multiple disciplinary approaches, appropriate to the project.
- There must be at least three researchers (including the Project Leader and Co-leader) who are or are eligible to be Principal Network Investigators within the GRAND NCE.
- There must be at least one Project Champion personally involved in planning and carrying out the project who is affiliated with a current or potential GRAND Partner drawn from the receptor community.
- One or more Partners from the receptor community must commit to making significant cash or in-kind contributions to the project.
- A current NSERC Form 100, SSHRC CV, or CIHR Common CV for both the Project Leader and Co-leader must be submitted as attachments to the LOI. Failure to include these attachments will be cause for immediate rejection.

Detailed instructions for completing this LOI template are on Page 2. More information on Phase 2 of the GRAND NCE is available on the GRAND website at the following URL, which will be updated with links to additional information as it becomes available: http://grand-nce.ca/renewal

Please note: If you complete this form using Preview, do not enter more text than is visible within the dimensions of the provided text box. Text that exceeds the visible limits will not be reviewed.

Project Title and Description

(●) Full project LOI ( ) Subproject only LOI

Title of proposed project
Literacy in New Media Privacy and Security

Brief description for public use
Much of life is now online, but privacy and security in this new landscape continue to be challenging. We propose that the key problem is a lack of shared literacy. We propose a multi-disciplinary approach involving social scientists and technologists working together to create a framework for shared understanding of the landscape, and a shared language for citizen engagement about the challenges and solutions.

Proposed Project Leader

(☑) Form 100, SSHRC CV, or CIHR CCV has been attached

Name	Email
Robert Biddle	robert.biddle@carleton.ca
University Carleton University	Title/Position Professor of Cognitive Science and Computer Science

Proposed Project Co-leader

(☑) Form 100, SSHRC CV, or CIHR CCV has been attached

Name	Email
Jacqueline Burkell	burkell@uwo.ca
University (must be different from Project Leader) University of Western Ontario	Title/Position Assiociate Professor of Information and Media Studies

Proposed Project Champion

( ) Confirmed ( ) Contacted (●) Not Yet Contacted

Name	Email
Michael Geist	Michael.Geist@uOttawa.ca
Organization University of Ottawa	Title/Position Canada Research Chair in Internet and E-commerce Law

Instructions for Letter of Intents for Phase 2 of the GRAND NCE

Front Page: All fields are mandatory. (a) Provide a project title and indicate whether the LOI is for a full project with subprojects or is only for a single subproject. LOIs that only propose a subproject will be matched with related LOIs to form full projects. (b) Provide a brief description of the proposed research suitable for posting on a public website that explains the project in terms accessible to the digital media community. (c) Provide the name, email address, university, and title for both the proposed project leader and the proposed project co-leader. (d) Provide the name, email address, organization name, and title for the proposed project champion (a person affiliated with a project partner who will be engaged in planning the project) and indicate whether the project champion has been confirmed, has only been contacted, or has yet to be contacted.

This Page: Read all of the instructions for completing the LOI template before filling out any of the information on later pages.

In **Part A**, provide the names of up to six partner organizations, indicate whether each has been confirmed, has only been contacted, or has yet to be contacted, and provide a brief explanation for how each organization will be involved in the project either as an active participant or as a potential receptor that will benefit from the research.

In **Part B**, list all GRAND projects that are related to the new LOI and also any other LOIs you are aware of that may be relevant to the new LOI.

In **Part C**, list up to nine additional co-applicants (not including the individuals listed on Page 1) who are expected to be involved as active participants in the research project. Indicate for each whether the individual is a project champion from the receptor community or an academic researcher.

In **Part D**, succinctly summarize (up to one half page) the problem being solved by the research.

In **Part E**, provide an overview (up to one and one half pages) of the proposed solution and the approach that will be taken in the research. Include relevant details about the theoretical framework, significant previous work, methodological approaches, and how the research will be managed and structured to achieve the desired goals. If you checked the box on the **Front Page** indicating you are submitting an LOI for only a subproject, just use the first box for **Part E**, don't use the second box on the continuation page.

In **Part F**, describe up to six subprojects (up to one half page for each subproject) that will be pursued during the first two years of the project. Indicate for each subproject the research question(s) that will be addressed, the relationship of the subproject to the rest of the project, the deliverables and assessment criteria appropriate for evaluating the success of the subproject, and the time frame (start and finish dates) estimated for the subproject. If you checked the box on the **Front Page** indicating you are submitting an LOI for only a subproject, enter "**N/A**" in all of the fields in **Part F** and continue to **Part G**.

In **Part G**, explain the likely technology transfer, knowledge mobilization, knowledge translation, or other activities that are planned for the project and how they may provide benefits to the receptor community.

In **Part H**, explain how the project will interact with other projects and the ways in which it may support or otherwise enhance the overall impact of the network.

In **Part I**, explain specific ways in which current or future partners will participate in the project and the mechanisms that will be used to ensure that this takes place.

In **Part J**, for each of the seven GRAND Challenges check whether the project will make its primary research contribution (check exactly one box) or a secondary research contribution (as many additional boxes as apply) to the challenge. Check "**N/A**" for any challenge that is not significantly impacted by the proposed research. For each challenge where a contribution is expected, provide a brief description of the likely contribution and its importance to the receptor community. The "Other" category may be used to describe anticipated contributions to the research infrastructure and enabling technologies and methodologies used in the GRAND NCE, or to other areas relevant to digital media that may be impacted, if the proposed research is expected to make a significant contribution in these areas.

Part A: Receptors and Partners list up to six organizations

Organization	Confirmed	Contacted	Not yet contacted
Office of the Privacy Commisioner of Canada	☐	☑	☐

Brief description of involvement

The OPC oversees compliance with the Privacy Act, which relates to Government acivity, and the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's private sector privacy law. We will work with them to better understand the priorities they see, and how improved literacy about privacy and security could help compliance, public education, and open discussion of the issues.

Organization	Confirmed	Contacted	Not yet contacted
CGI Inc.	☑	☐	☐

Brief description of involvement

CGI is now Canada's largest IT company, with a focus on services and infrastructure management and cloud computing. We will work with them on new and better tools for security operations centre management.

Organization	Confirmed	Contacted	Not yet contacted
CA Technologies	☑	☐	☐

Brief description of involvement

CA Technologies is a Fortune 500 company with offices across Canada. It's primary focus is on software for enterprise infrastructure management. We are working with CA doing design work for improved tools for operator attention and collaborative vigilance and problem solving in managing cloud computer security.

Organization	Confirmed	Contacted	Not yet contacted
Ministry of Public Safety	☑	☐	☐

Brief description of involvement

The Federal Ministry of Public Safety is responsible for coordinating Canada's Cyber Security Strategy. with the main objectives of the Strategy are to secure government systems, work with others to secure systems outside of government, and help Canadians to be safer online. We will work with them on strategies for public education and discussion about cyber-security.

Organization	Confirmed	Contacted	Not yet contacted
MediaSmarts	☐	☑	☐

Brief description of involvement

MediaSmarts is a Canadian not-for-profit charitable organization for digital and media literacy. They develop digital and media literacy programs and resources for Canadian homes, schools, and communities. The research and policy outcomes from this sub-project will inform the development of associated literacy resources.

Organization	Confirmed	Contacted	Not yet contacted
	☐	☐	☑

Brief description of involvement

Part B: Relations to existing and proposed projects in the GRAND NCE

Related Current Projects

PRIVNM (current privacy project) , SHRDSP (shared displays have implications with privacy and management), DIGLT (games are an important new form of media for literacy), NEWS (for citizen engagement on privacy).

Related LOIs

SHARE (proposed successor to SHRDSP), SEGAVIWO (proposed successor to DIGLT), NEWS

Part C: Additional Co-Applicants List up to nine additional co-applicants		
Name Sam Trosow	Email strosow@uwo.ca	☐ Project Champion ☑ Researcher
Organization University of Western Ontario	Title/Position Assoc. Prof. of Law and IM Studies	
Name Barry Wellman	Email wellman@chass.utoronto.ca	☐ Project Champion ☑ Researcher
Organization University of Toronto	Title/Position Professor of Sociology	
Name Sandrine de Ribaupierre	Email sderibau@uwo.ca	☐ Project Champion ☑ Researcher
Organization University of Western Ontario	Title/Position Asst. Prof. of Neurosurgery	
Name Anabel Quan-Haase	Email aquanhaa@uwo.ca	☐ Project Champion ☑ Researcher
Organization University of Western Ontario	Title/Position Assoc. Prof. Information Media Studies	
Name Valerie Steeves	Email Valerie.Steeves@uottawa.ca	☐ Project Champion ☑ Researcher
Organization University of Ottawa	Title/Position Associate Professor of Criminology	
Name Sonia Chiasson	Email chiasson@scs.carleton.ca	☐ Project Champion ☑ Researcher
Organization Carleton University	Title/Position CRC Human Oriented Computer Security	
Name Konstantin Beznosov	Email beznosov@ece.ubc.ca	☐ Project Champion ☑ Researcher
Organization University of British Columbia	Title/Position Assoc. Prof. Electtrical & Computer Eng.	
Name Kirstie Hawkey	Email hawkey@cs.dal.ca	☐ Project Champion ☑ Researcher
Organization Dalhousie University	Title/Position Asst. Prof. of Computer Science	
Name Jason Nolan	Email jnolan@ryerson.ca	☐ Project Champion ☑ Researcher
Organization Ryerson University	Title/Position Asst. Prof., Early Childhood Development	

Part D: Summarize the problem being solved (1/2 page)

Although much of life is now online, and as a society we are increasingly familiar with the online environment, privacy and security in this new landscape continue to be challenging. The opportunities associated with the collection and analysis of personal information online are significant, with impacts on commerce (from manufacturing to retail), social life (from friendship to families), and government (from voting to peacekeeping). But, as we have taken advantage of these opportunities, privacy protection and data security have not kept pace: indeed they have become weaker. Challenging security, there are intelligent and adaptable adversaries at work. Challenging privacy, there are commercial and government agencies interested in framing software to reveal behaviour and relationships. Industries endeavour to increase competitiveness, but in ways that can promote risk for themselves and their clients; governments compromise personal privacy in the interests of public security. Legal frameworks that regulate privacy and security are not easily applied in the online environment, where there are no borders and no universal social consensus, and legislators struggle to adapt established models to the new frontier. Individual vigilance is not a viable response to these challenges, since the technologies and strategies that undermine privacy and security change with astounding rapidity. Furthermore, even where there is technology and/or legal frameworks that can help, too few people understand them or use them. Many have worked to improve matters, but with limited success. We propose that the key problem is a lack of shared literacy. Individuals do not have a good understanding of privacy and security threats; nor do they understand the defenses against these threats. Too often, the response to privacy and security challenges is vague and simplistic advice, unrealistic requirements, and a public sense of 'dread risk'. Users are exhorted to 'change passwords often', 'watch out for password phishing', and 'avoid identity theft'. We need a new approach. The responsibility for personal privacy and data security must be shared between the general public, the government, commercial organizations, and other stakeholders. We need to build a shared understanding of privacy and security issues that incorporates the perspectives and interests of various stakeholders. We need to establish communication between the stakeholder groups, and address privacy and security challenges in the context of this shared communication. We need to distribute the responsibility for privacy and security, so individuals do not bear the full weight of ensuring their personal privacy and the security of their online information. Ultimately, we need to establish common privacy and security principles, develop a common language to talk about these issues, establish clear goals, and develop plans for the improvement of online privacy and security.

Part E: Summarize the proposed solution and approach (1 ½ pages)

We propose that the way to address privacy and security in the online world is to promote widespread *literacy*. By literacy, we mean a shared understanding of the landscape, and a shared language for citizen engagement about the challenges and solutions. We propose a multi-disciplinary approach involving social scientists and technologists working together.

In our project, we propose to use the idea of literacy in several ways. We will conduct research on citizen understanding of privacy and security, the state of the art, and the state of expectation. We will promote understanding of the law and of evolving social practice as it relates to privacy and security. We will explore technology weaknesses and strengths for privacy and security, and make them known. We will explore technology to promote literacy about privacy and security implications of the technology itself. We will work with all other projects within GRAND, to identify the challenges for privacy and security in the scope of those projects, because we ourselves in GRAND must be literate about the privacy and security implications of our own work.

In the Social Sciences, a wide variety of literacies have been proposed for online environments, including information literacy (Association of College and Research Libraries, 2000), computer literacy (Tellis, 2009), media literacy (Potter, 2012), and many others. There is widespread debate on scope and relevance of each of these literacies (see, e.g., Bawden, 2008), and the various concepts show significant overlap as well as differences in scope and emphasis. Each of these various conceptions, however, includes some aspects of information management expertise among the identified literacy requirements or skills. Standard Five of the ACRL Information Literacy Competency Standards for Higher Education (2000), for example, reads: The information literate student understands many of the economic, legal, and social issues surrounding the use of information and access and uses information ethically and legally. Manguson (2011) identifies online privacy and reputation management as information literacy skills. Cooney and Hiris (2003; see also Katz, 2007 and O'Hanlon, 2002) explicitly evaluate user understanding of fair use, copyright, and citation in their study of information literacy among business students. Joint (2006) argues that intellectual property rights should be part of the information literacy syllabus, while Warren and Duckett (2010) suggest that information literacy training should address the economics of information.

Part E: Summarize the proposed solution and approach (continued, but only for full project LOIs)

Computer literacy courses include discussion of copyright and intellectual property issues (Hoffman and Blake, 2003). The Norwegian Directorate for Education and Training (as cited in Lankshear & Knobel, 2006, p. 120), notes that digital literacy skills "involve being aware of the protection of privacy and intellectual property rights and applying and adhering to rules and norms for Internet-based communications", and the Media Awareness Network (2010, p. 5) indicates that digital literacy skills include "information management skills and an appreciation of ones rights and responsibilities with respect to intellectual property." Media literacy, which is typically focused on informed consumption of media products, includes an emphasis on privacy, "to help youth develop the knowledge and skills they need to better manage their personal information online" (MediaSmarts, 2012). Thus, across different terminologies, domains, and literatures, one important and consistent theme arises: effective negotiation of the digital environment requires the skills and knowledge to manage information. In the current information environment, the information management skills required to legally and ethically obtain information, interpret regulatory frameworks, understand consent documents, and utilize the tools available to protect user data are core competencies for informed citizenship.

Technology to support privacy and security has a long history with some important contributions that still have much to offer. While many of these contributions have strong scientific underpinnings, they have poor human-factors design, and the result is that they are commonly misunderstood, misused, or unused. Much of the technology is based on asymmetric encryption, where one "key" is used to encode information, and a different key is used to decode the information. This structure can support important services, such as private email, and verifiable identification of the origin of software downloads. Sadly, both are still widely unused because of poor human-factors design: people do not understand them, nor how to use them. Even technologies such as passwords or access control are widely misunderstood, with the result that people use weak passwords, and accidentally allow unintended people access to private information. These are only a few examples, but the general picture is clear: we need to make software that supports privacy and security easier to use. We see this as a literacy problem, and we see the potential being in the solution in the design of the software. Essentially, we suggest privacy and security software should signal how they are to be used, and the effect they will have. The theoretical models that support this are Gibson's theory of affordances, and the Fischoff's mental model theory of risk and safety. Reeder's work at CMU and Microsoft (Reeder et al. CH2012) shows how Access Control can be made more understandble. The usage and intent should be implicit and visible in the design itself.

For our "champion", we propose someone as more a "challanger": Prof. Michael Geist at the Univesity of Ottawa. Geist is Tier 1 Canada Research Chair in Internet and E-commerce Law, and is a member of the Advisiory Board of the Electronic Frontier Foundation. He is known across Canada as an advocate for understanding and reform for privacy and rights in cyberspace through his research work, his media appearances, and his regular newspaper columns. We propose that Geist issue challenges to our project researchers to keep our project priorities in focus. We have not yet proposed this to him, pending approval of this unusual idea.

We also propose to serve GRAND itself, and GRAND projects. Our work is on literacy on privacy in new media, and we propose to survey and engage on the privacy and security implications of every GRAND project. To do this we propose to work with NAVEL, or its successor project (the leader of NAVEL, Wellman, is a member of our PRIVLIT project). In this way we can leverage the NAVEL contact structure, and provide reports to GRAND itself on our reflection, jointly with each project's members, on new media privacy issues. Moreover, by taking this approach, we will ensure that we shine the light on ourselves, not merely outsiders, to critically engage on issues about privacy in new media.

To conclude our proposal, we wish to outline the cross-disclipinary lessons we have learned in our earlier GRAND work, and how they inform this proposal. Our earlier project was PRIVNM (Usable Privacy and Security in New Media), and we had a balance of researchers from Computer Science and the Social Sciences). We found a tendancy for the Computer Scientists to focus on attempting to solve current problems, and a tendency for the Social Scientists to identify new problems; we would prefer to engage with each other more closely. We have chosen our new approach - literacy - as a common cause to which we can both contribute.

Part F: Subprojects list up to six subprojects that will be undertaken in the first two years (only for full project LOIs).

Subproject Name (1)

Privacy in the Digital Memory Revolution (Wellman, Quan-Haase, McEwen, Nolan, Burkell)

Summary

Our research into the interplay between physical and digital memory objects builds on our studies of the processes, reasons and structural outcomes for behaviour in the age of the internet: online social networks, the far-flung personalized internet, and mobile communication and information. Our focus is to understand the kinds of memories that contemporary individuals and households wish to keep in physical, digital and hybrid form. We are especially interested in how Canadians balance both digital access to their digital memories and their concerns about keeping their memories controllably private. In a group society, people were either in or out of a densely knit set of broadly encompassing relations: communities, work groups, civic organizations. By contrast, in a networked society, people do not belong to one group but have partial memberships in a variety of more weakly bounded networks. They lose the security (and control) of the group-centered society, and they must actively create a social network on their own. Many services are promoted for self-awareness by personal logging of real-world activities: pedometers and wearable cameras. Less obvious issues with these are the psychological implications of these digital memories. Research in autobiographical memory suggests that it is necessarily incomplete: our identities depend on being able to construct a coherent life narrative, which in turn depends on the ability to 'edit' autobiographical memory to be consistent with that narrative. Our work in all these aspects of digital memory will feature field studies to document actual lived experience to better inform public discourse.

Subproject Name (2)

Understanding Privacy and Security in Online Social Networks (Steeves, Burkell, Beznosov, Quan-Haase)

Summary

Social network software involves people identifying personal details and relations, and these can be easily be exploited. We propose two lines of research. One, headed by Steeves of the University of Ottawa, explores issues surrounding discrimination, such as gender, attractiveness, age, race, or any number of other characteristics. We will focus on gender-based harassment, discrimination, and judgement that girls and women experience in the off-line world reappear in the online social environment, at times under new guises and with new intensity. We will explore the experience of girls in online social networks, and examine the ways in which 'girls online' are constructed in academic and policy discourses. Our goal is to develop new knowledge about the ways in which girls and young women incorporate digital media into their lives and use that knowledge. A second approach, under the direction of Beznosov, is to explore general attack strategies that make it feasible to design "socialbots" that "sense," "think," and act cooperatively in social settings, just as in social robotics. In the wrong hands, such socialbots might be used to infiltrate online communities, build up trust over time, and then send personalized messages to elicit information, sway opinions, and call to action. In this research, we plan to perform a security analysis of malicious socialbots. While the motivations for operating socialbots and the technical mechanisms that enable them remain rich areas of research, we focus on studying their malicious behavior and developing countermeasures.

Subproject Name (3)

Privacy of Personal Health-Related Information Sharing (Beznosov, de Ribaupierre, Burkell)

Summary

Initially, online privacy was explored mostly in the domain of electronic commerce, but more recently the attention of both media and researchers has focused on more personal aspects, such as health-related information. Privacy and confidentiality are concerns for end-users, who may not want their personal details to be shared with untrusted third-party entities in personally identifiable ways. But issues also arise for experts and professionals, who may wish to share and consult to best perform their role, but who wish to ensure that privacy expectations of all parties are met. Further, information content providers may not wish to make all their material openly available, but on an as-needed basis for specifics, with other information available only in aggregate form. We need to develop empirically-grounded understanding of the above requirements by conducting qualitative and quantitative studies of the stakeholders' privacy-related attitudes, concerns, and needs in the context of health information sharing. We then propose to develop a framework for making the issues and implications clear to everyone, and to explore software systems to shape and protect access to support heath information sharing where desirable, but protect privacy and confidentiality as necessary.

Part F: Subprojects (continued, only for full project LOIs)

Subproject Name (4)

Legal Literacy and Personal Data Collection (Trosow, Biddle)

Summary

The surveillance and collection of Canadians' intellectual property and personal data occurs daily. This sub-project aims to explore the absence of legal literacy in the way that individuals interact with information-extracting hardware and software, and the subsequent power this provides to companies and institutions. In particular, the project explores the privacy implications of three digital technologies: anti-plagiarism software, social network and mobile application waiver forms and gaming consoles. Social network membership and mobile application downloads often come with significant waivers that force users to choose between waiving their privacy rights and not using the network service or application. In practical implementation, most consumers simply skip the lengthy and legalese-heavy contracts and thus never learn about the rights and personal information they are giving away.
There are pedagogical, political and legal issues in all these: privacy rights, copyrights, software efficacy, the effect on the learning experience, and what role laws play, such as Fair Use regulation or the US Patriot Act. This research program seeks to chronicle the issues from both a legal and pedagogical perspective. We will also uncover the most common rights waived to join social networks or download apps. We will also explore how people understand the personal data they are disclosing, and will determine the best practices for creating "contract equivalencies", a new movement to provide a layperson-friendly version alongside the legal contract.

Subproject Name (5)

Privacy/Security Awareness Design (Biddle, Chiasson, Hawkey)

Summary

Many software applications and parts of applications specifically support privacy and security. These include Password systems, Anti-Virus systems, and Access-control systems. Such software exists to support the user in protecting themselves online. The engineering infrastructure is typically strong, and is the basis of much research and development over recent decades. But the software often fails because the human factors design is weak, and people do not understand how to use the software, what the threats are, and how the software supports defence. It is common for users to ignore, misuse, or bypass, all because of this weak design. We believe it is possible to address this by leveraging knowledge of human understanding and human behaviour, using the design itself to leverage human strengths and to help users build good mental models. In particular, this new approach to design can use graphics and animation to support these improvements. Our work on graphical passwords (Biddle et al. 2012) shows what has been learned in the area of authentication, and we propose to continue this work on other privacy and security supporting software. We will apply our knowledge of human factors and learning mental models, use our design skills and human-factors quantitative and qualitative methods to evaluation our work. Our immediate agenda includes password managers, mobile device security, and anti-virus software. We will also extend this work to software for managing privacy and security in the clould, addressing the design of software used in operations centres where security is monitored.

Subproject Name (6)

Perspectives and Attitudes about Covert Surveillance (Burkell, Quan-Haase, Biddle)

Summary

With the recent leak by Edward Snowdon that reveals the systematic harvesting and analysis of internet metadata by US security agencies, covert surveillance has once again become big news. Some view Snowdon as a renegade criminal for exposing surveillance systems; others view his as a "amazingly brave and courageous act of civil disobedience." (The Guardian, Wednesday June 12, 2013). Each stakeholder, including the general public, policy makers, software and hardware developers, security experts, and users of covert surveillance, brings particular knowledge and perspective to the issue. The goal of this project is to uncover and describe these various subjective understandings using a combination of interview/focus group, content analysis, and survey techniques. The results of this research will be educational and policy materials that bridge the gaps between the stakeholder groups, providing an understanding of common ground and unique perspectives. More generally, we propose to study attitudes to the issues on privacy and security in different communities that have key roles. In particular, we will study the computer security community itself in order to describe the human attutudes and forces at work in providing the enabling technical infrastructure for surveilance and defence against it.

Part G: Summarize how the proposed project will pursue knowledge and technology exchange and exploitation activities within the context of GRAND.

Our main work, across all sub-projects, will involve publication of research as a primary method of making the results of our work available. In addition to that, we will work with our industry and government partners, providing them with advice from our research. For example, for our government partners, potentially the Office of the Privacy Commisioner and the Ministry of Public Safefy, we will provide our results on better undertstanding the issues of privacy and security in new media, and our advice on how to leverage this knowledge in public education and citizen engagement. For our industry partners, we will provide our results on software design for both end-user and clould privacy/security management. We also hope to bring our government and industry partners together to work towards a common language and a commone framework for advancing literacy on new media privacy. With their help, we then hope to facilitate direct citizen engagement.

Part H: Summarize how the project will network with other projects within GRAND.

There are two ways in which we propose to work with other projects in GRAND.

Firstly, we wish to coordinate some sub-projects in other projects that relate directly to furthering privacy and security literacy. For example, SHARE (formely SHRDSP) has a proposed sub-project on collaborative sense-making, with privacy and security management as a specific example. SEGAVIWO (formerly DIGLT) has sub-project on games to build mental models, with security and privacy understanding as specific examples. NEWS has a special role in promoting literacy as the foundation for an informed citizenry.

Secondly, we wish to survey and engage with all projects across GRAND to indentify and discuss the privacy and security implications that may arise in other the systems they study.

Part I: Summarize how one or more current or potential GRAND partners will be engaged in and benefit from the proposed research.

Office of the Privacy Commisioner of Canada: will be consulted with and reported to, will be able to leverage results for public education.

Ministry of Public Safety: will be consulted with and reported to, will be able to leverage results for public education.

MediaSmarts: will be informed by research and policy outcomes for development of associated literacy resources.

CGI Inc.: will work with us on field studies of cloud security/privacy management, and be able to use our results and designs.

CA Technolgies: will work with us on field studies of cloud security/privacy management, and be able to use our results and designs.

Part J: GRAND Challenges Check all that apply and briefly describe anticipated impact	
Entertainment ❍ Primary impact ❍ Secondary impact ◉ N/A	
Learning ❍ Primary impact ◉ Secondary impact ❍ N/A	Our main aim is literacy, and an important aspect is supporting the literacy by learning; everyone online should learn about the systems they use and their privacy implications. We hope to design systems that faciliate this.
Healthcare ❍ Primary impact ◉ Secondary impact ❍ N/A	As healthcare information become more online, so the issues of privacy and security become more important. We need to study and understand how desirable health information sharing can be accomplished without losing control.
Sustainability ❍ Primary impact ❍ Secondary impact ◉ N/A	
Big Data ❍ Primary impact ◉ Secondary impact ❍ N/A	Private information might seem to be protected, but "big data" analysis might potentially allow private information to be revealed through cross-linkages and inference. Moreover, some systems may encourage private data to be revealed in order to build "big data" for analysis of large trends.
Work ❍ Primary impact ◉ Secondary impact ❍ N/A	It is now common for the workplace to overlap with private lives, and for private data to be monitored or utilized by employers or governments. We need to understand the issues, and how the wishes of workers and industry might work together: there is a power imbalance that makes the issue difficult but especially important.
Citizenship ◉ Primary impact ❍ Secondary impact ❍ N/A	This is our primary theme. It is our intention to identify, understand, and support the literacy that is needed about privacy and security. This literacy is the essential underpinning for citizen engagement on the critical topics of privacy and security in new media. At the same time, many of the systems we study, such as social networks, are themselves now part the infrastructure of citizen enagement.
Other ❍ Primary impact ❍ Secondary impact ◉ N/A	