July 13, 2016

The Office of the Privacy Commissioner of Canada
30 Victoria Street, 1st Floor
Gatineau, QC K1A 1H3

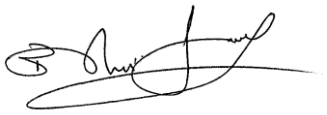
Re: Response Submission to Consultation Paper on Consent and Privacy

The Canadian Information Processing Society (CIPS) respectfully submits our response to your May 2016 discussion paper that explores potential enhancements to consent under PIPEDA. Founded in 1958, CIPS is an association of information technology professionals with representation across Canada. We have read and understood the consultation procedures; we thank you for this opportunity.

Our submission, including a one-page summary, is attached. Please note: CIPS is not subject to the Official Languages Act, thus our response is submitted in English only.

We wish you much success in your important work. We look forward to the opportunity to discuss our submission further with your Office.

Sincerely,



Bashir Fancy, I.S.P.
Chair, CIPS National Board

Contact for this submission is:

Mary Jean Kucerak, CAE
Chief Operating Officer
CIPS National
5090 Explorer Drive, Suite 801
Mississauga, Ontario L4W 4T9

Phone: (905) 602-1370
Toll Free: 1-877-ASK-CIPS (275-2477)
Fax: (905) 602-7884
E-mail: mj@cips.ca

Canadian Information Processing Society (CIPS) Submission to the Office of the Privacy Commission of Canada Discussion Paper on Consent and Privacy

Respectfully Submitted: July 13, 2016

Summary

Culture and society are changing, along with rapid advancements in information and communications technology. CIPS members are proud to be key contributors to these advancements across Canada and internationally. Our members recognize roles are shifting to further include global thinking, data provenance, social policy, and legal and ethical concerns. As the boundaries of our members' roles change, the need for the boundaries of the Office of the Privacy Commissioner of Canada (the "OPC") also needs to change.

Our response outlines the issues and opportunities CIPS would like to see as priorities for your work in privacy and consent. We believe:

- a framework is required that establishes a holistic privacy and consent solution; Privacy by Design must be an integral part.
- there is a need for all IT practitioners … a vital part of Canadian business and the day-to-day lives of Canadians… to uphold professional standards that incorporate certification, legal education and ethical standards, overseen by an independent body. [CIPS has had this kind of mechanism in place since 1989. Our professional designation, the *I.S.P.*, provides a model for your consideration, with the potential to establish IT practitioners as fundamental to upholding privacy and consent legislation. The hard work of securing recognition in law for the I.S.P. by six provinces across Canada has been already accomplished by CIPS.]
- a governance model is necessary that holds senior decision–makers in organizations accountable for standards that rigorously safeguard privacy rights of all Canadians
- there is a need for legislative change to provide the OPC with greater powers to help ensure Canadians' privacy is protected in our increasingly complex world.

We thank you for your efforts to-date. We hope our input is influential on your next steps. We are confident in the ability of our members to contribute, in a highly meaningful way, to the continuing conversation:
---shaping the rules for collection, use and disclosure of personal information in Canada.

Table of Contents

Introduction

Thank you for the opportunity to read, reflect upon and respond to your thoughtful and important document on consent and privacy. The Canadian Information Processing Society (CIPS)[1], is Canada's national professional association for Information Technology practitioners. Our members provide leadership, interpretation of and operational involvement with national and where-applicable, provincial privacy legislation.

We support your ongoing efforts to identify and prioritize strategic privacy priorities in our complex and fast-moving world. We thank you for the opportunity to respond to your discussion paper on privacy and consent, released in May 2016; the scope of our thoughts and responses have been limited to the mandate of CIPS. (Appendix A.)

In the Introduction section of your document, you indicate some prior discussions with stakeholders have included feedback questioning "…the continued validity of the consent model in an ecosystem of vast, complex information flows and ubiquitous computing."

CIPS believes these very points increase the need for greater emphasis and scrutiny of the evolving meaning of consent in privacy protection. At the same time, we believe major shifts are needed in how organizations, the public and your Office interpret and apply consent and privacy rules in their business and daily lives. These are global issues; as Canada's representative to the leading international IT organizations,[2] CIPS is very capable of considering these implications,[3] (Appendix B), while focusing on the needs of Canadians today and into the future.

We hope our input is useful for your next steps. We have valued the opportunity to discuss these important issues internally. We look forward to the opportunity to continue this conversation with your Office.

Scope of Our Response

Your discussion paper provided CIPS with many points for consideration and discussion. We have limited our response to those areas that best fit within the mandate of CIPS. Beyond the mandatory response to at least one consultation question, we have taken the opportunity to

[1] http://www.cips.ca/
[2] http://www.ifip.org/
[3] http://ipthree.org/

respond to a few of the reflection questions that are again, a strong fit with our mandate.

Our response is relatively brief: we anticipate your Office will receive a substantial number of responses and, we hope our response is only the beginning of deeper communications between our two organizations.

Reflection Questions

The reflection questions interspersed throughout the discussion paper provided our organization with an opportunity to discuss many of the challenges in privacy and consent. Brief perspectives are shared below.

What measures have the potential to enhance consent? How should their development / adoption be promoted?

We agree with Privacy Commissioner Therrien's statement the "…personal consent model is under significant stress."[4] Greater transparency in privacy policies and notices is not enough. We believe the OPC needs to look beyond issues that are really distractions … difficult legal language, lengthy policies, small display screens on devices, just-in-time consent for wearables and the lack of real opportunity for consent in the Smart X[5] world[6], in order to better protect the privacy and dignity of Canadians.

The complexity of the technical environment continually increases. We cannot expect most Canadians have either time or interest to understand sophisticated technologies, nor the potential algorithmic profiling, harvesting, and selling of data, in order to provide meaningful consent. In particular, the Internet of Things, (IoT) along with blockchain applications such as 'self-executing contracts,' will challenge the traditional consent model.

Unfortunately, penalties applied to organizations that misuse data (for example ignoring the scope of consent given) have proven to be weak deterrents[7]. Succinctly stated – we believe neither individual Canadians, nor regulations, can 'keep up' with entities that directly collect

[4] From 2016 IAPP Canada Privacy Symposium speech delivered by Privacy Commission Daniel Therrien
[5] Smart X includes but is not limited to: smart cities, smart buildings, smart homes
[6] Edwards, Lillian (2016). Privacy, security and data protection in smart cities: a critical EU law perspective, University of Strathclyde, Glasgow
[7] Pasquale, Frank (2015). The Black Box Society. Secret algorithms that control money and information. Harvard University Press, London, England.

data, obtain data through a third party or aggregate data. Therefore, professionals and professional entities need to 'step up' to the challenge of safeguarding privacy, implementing fair consent practices and enabling effective regulatory oversight. As your document states, "…privacy protections, including meaningful consent, [need to be]…'baked in'. This approach supports a 'privacy by design' governance model.

Should consent be required for the collection, use and disclosure of de-identified data? If so, under what conditions? Is there a workable, risk-based approach that can vary the stringency of the consent requirement with the risk of re-identifiability of data?

The absence of personal information in data does not necessarily protect an individual's privacy. We believe there should be no exceptions to obtaining meaningful consent. A number of scientific and legal studies support our viewpoint, based upon the inability to guarantee data cannot be re-identified. Even with technological advances in de-identification approaches, there always remains a method to remove anonymization. Paul Ohm's (2010) article in the UCLA Law Review remains relevant today and conveys many of our concerns[8]. The article concludes with: "Regulators must respond rapidly and forcefully to this disruptive technological shift, to restore balance to the law and protect all of us from imminent, significant harm. They must do this without leaning on the easy-to-apply, appealingly non-disruptive, but hopelessly flawed crutch of personally identifiable information."

Fortunately, work published by Rubinstein and Hartzog (2016)[9] has provided a risk management approach based on '...reasonable adherence to industry standards'. This article discusses the merits of a data release policy and associated processes in order to minimize data re-identification risks. These ideas would require proper education and governance models for technology and data practitioners; CIPS supports this promising approach.

How should such ethics boards be created, composed and funded? Who should they report to, and what should be their decision-making authority?

Ethics boards could oversee the adherence of ethical principles by select key practitioners, including a defined set of behaviour and knowledge and skill competencies. This approach supports the notion "…we must build structures that encourage ethical data usage, rather than merely nudging individual consumers into sharing as much as possible, for as little as possible,

[8] Ohm, Paul (2010). Broken Promises of Privacy: Responding to the surprising failure of anonymization. UCLA Law Review 57, pp 1701-1777.

[9] Rubinstein, Ira & Hartzog, Woodrow (2016). Anonymization and Risk. Washington Law Review, Vol 91, No 2

in return"[10]. CIPS has had this kind of mechanism in place for many years. CIPS members commit to a rigorous code of ethics. Certified members (I.S.P. and I.T.C.P./IP3P) are subject to peer review and disciplinary reviews for misbehavior. This can result in the loss of their CIPS certification. The process is overseen by peer-staffed, discipline review committees.

As indicated in your discussion paper, these boards face the challenge of having little or no meaningful power. Another consideration is the scope of the proposed board; although potentially modelled on academic research ethics boards, this approach may be too narrow.

For example, secondary data research requires research ethics board approval at Canadian post-secondary, academic institutions. The research does not consider if consent was given for this particular use of the data since it is within the 'research' mandate of PIPEDA. This will be increasingly complex for a board when considering secondary data, public data and so forth, within a non-academic context. Some even suggest it will be impossible to scope the work of the board so it is completed within a reasonable period of time, by individuals technically able to understand data source, consent, and so forth.

Long-standing tradition calls for ethics boards to be composed of a combination of experts and "typical users" impacted by the board's decisions. So, for example, medical ethics review boards often are often composed of both medical researchers and volunteer members of the community. Councils overseeing professional engineers across Canada also follow this approach. This approach may be fruitful with the proviso, effort must be made to ensure a reasonable representation of the range of "typical users" from the perspectives of technological literacy, age, cultural and other factors.

Funding for such boards could come from the entity that wants to use personal data; they will pay an annual fee to be "Trust Marked" by this ethics body. Already in place, well recognized and respected in Canada is the CSA Group mark[11] and this can provide a model for going forward. In seeing this mark, individuals know the holder is actively working to protect their information.

[10] Richards, Neil M. & King, Jonathan H. (2014). Big Data Ethics. Wake Forest Law Review (49), pp 393-432.
[11] http://www.csagroup.org/

Consultation Questions

#1. Of the solutions identified in this paper, which one(s) has/have the most merit and why?

#2 What solutions have we not identified that would be helpful in addressing consent challenges and why?

We have combined our response to your questions #1 and #2 as follows: The Privacy by Design (PbD) approach is, we believe, key in moving forward with enhancements to privacy and consent under PIPEDA. However, PbD is part of a larger framework that establishes a holistic privacy and consent solution. We believe this definition comes close to describing the holistic perspective: "*Privacy by Design (PbD)* is an approach to protecting privacy by embedding it into design specifications of technologies, business practices, and physical infrastructures.[12]"And PbD must become part of an organization's DNA. However, we recognize there is a huge gap to close to reach this goal. Looking beyond technologies such as coding PbD into new or updated applications and associated services, we would like to see the following components included:

a. Professional certification: Similar to the mandatory certification requirements of the Canadian financial services industry, professionals involved in the management of information resources including, but not limited to, applications development, applications support, data architecture, data analysis, process analysis, IT management, IT sales, IT education, Chief Data Office (DCO) and Chief Information Officer (CIO) need to be certified in a minimum level of privacy and consent laws and best practices. An example to consider is the need for most employees in financial services to have at least a minimum level of education in anti-money laundering. This training is required on a bi-annual basis, tracked by employers and available for audit by regulators. Results from a survey of software designers indicate "Many designers perceive privacy as a theoretical-abstract concept, rather than an applicable principle in designing information systems."[13] These results heighten our concern the IT industry is sorely lacking in key skills and knowledge. We have little reason to believe results would differ materially if a survey of Canadian software designers was undertaken. CIPS has a Common Body of Knowledge document in place, created as an integral part of our mandatory ongoing professional development. This could be further enhanced with more detailed education on privacy and consent, supporting the increasing risks in our industry.

[12] www.privacybydesign.ca

[13] Hadar, Irit and Hasson, Tomer and Ayalon, Oshrat and Toch, Eran and Birnhack, Michael and Sherman, Sofia and Balissa, Arod, Are Designers Ready for Privacy by Design? Examining Perceptions of Privacy Among Information Systems Designers (March 24, 2014). 2014 TPRC Conference Paper. Available at SSRN: http://ssrn.com/abstract=2413498 or http://dx.doi.org/10.2139/ssrn.2413498

This viewpoint is supported by the IP3 paper discussing transformation for the IT industry. It suggests the gap in knowledge outside of technology needs to be filled; IT professionals increasingly require a level of legal and commercial competence. Other professions have already taken this approach, including professional engineers and financial planners: each are required to complete initial ethics education, as well as continuing education, to uphold the ethics and integrity of their professions.

Of note, in 2014, CIPS implemented an (on-line) ethics examination for all applicants for CIPS' certification.

b. Governance and accountability: Pedro Domingos, when discussing machine learning and artificial intelligence in his book on technical designers and privacy, ponders accountability: "…personal data is used daily in the operation of even the most conservative of institutions – banks/credit card companies - and no humans are involved - how do we hold the machines accountable?"[14] The increasing complexity of data analytics and associated processes is growing rapidly within organizations of every size. An acceleration to compete and the associated complexity cannot distance the senior executives of an organization from its analytics and technology operations. Organizations need to be held accountable for privacy, and, proactively need to have in place governance that ensures corporate CEOs and executives recognize this within their mandate. Without accountability, risks paralleling the complexity of issues related to the global financial crisis arise: "When a CEO can step up to the witness stand and disclaim understanding of core actions of his/her own firm on the grounds of complexity, it's hard to imagine how basic legal principles of responsibility and fiduciary duty can endure."[15].

This accountability needs to begin with C level executives and Boards of Directors. It also must include employees and management who, through certification, are knowledgeable and responsible for privacy process and application. This point has been emphasized by a speaker at a recent cyber security conference in Toronto: "They're [upper management] not listening to us. They get it, they just don't need to do anything about it. They're accumulating technical debt. Every year they don't spend enough on information security, they're adding to the debt and hoping when the debt comes due they're not around to take the fall … The market should punish these people, just like they were accumulating financial debt… and they would go out

[14] Domingos, Pedro (2015). The master algorithm. How the quest for the ultimate learning machine will remake our world. Basic Books, New York, NY.
[15] Pasquale, Frank (2015). p 173.

of business."[16]

A Parliamentary committee in the UK in their recently released report on cyber-security is also recommending accountability at the executive level: "It is appropriate for the CEO to lead a crisis response, should a major attack arise. But cyber security should sit with someone able to take full day-to-day responsibility, with Board oversight, who can be fully sanctioned if the company has not taken sufficient steps to protect itself from a cyber-attack. To ensure this issue receives sufficient CEO attention *before* a crisis strikes, a portion of CEO compensation should be linked to effective cyber security, in a way to be decided by the Board."[17]

#3 What roles, responsibilities and authorities should the parties responsible for promoting the development and adoption of solutions have to produce the most effective system?

A coordinated approach across jurisdictions will produce the most effective system. We encourage your Office to review the IP3 report, "The GIC 2020 Skills Assessment[18]". As Canada's representative to IP3, CIPS participated in writing the report, along with other international stakeholders. Section 4.2.4 forms the regulation, risk and compliance section and an excerpt is below:

"Existing legislation and regulatory frameworks are unable to keep pace with the current introduction and adoption of new technologies. This is seen as the largest area of growth and challenge to the ICT industry professional. There are an ever increasing number of concerns as technology is adopted more fully in industries that have not typically used it. Technology is part of multi-agent systems and the risk is that legislation and regulation will be created in a fragmented, proprietary way that will inhibit the adoption of safe policy. This could enable the unscrupulous to take advantage.

Variation across governments and industries is inhibiting real progress and a simpler set of agreed to guidelines will drive innovation, job creation and ultimately improve lives."

#4 What, if any, legislative changes are required?

CIPS supports the OPC in seeking order-making powers in order to help ensure a proactive approach. As you consider legislative change, we ask you continue to collaborate with those provinces that have their own privacy legislation in place to ensure an effective pan-Canadian model. CIPS collaborates nationally, although we have distinct provincial boards; we recognize

[16] Murray, Jason, Senior Manager MNP LLP, SC Congress Conference, Toronto, Ontario, June 2, 2016
[17] http://www.publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/14812.htm#_idTextAnchor038
[18] Global Industry Council (GIC) 2020 ICT Skills Assessment, (http://ipthree.org/skills-2020-assessment-report/)

this can be a time consuming approach but always results in a superior outcome. We also recognize '….Globalisation will feature more within an ICT professional's thinking" and global agreements will be required to ensure respect of privacy and consent[19]. With this in mind, we also anticipate your office will seek out supportive global relationships to align with any legislative changes. We look forward to discussing these broad, important and timely issues further with your Office and other stakeholders.

CIPS Offer of Support & Next Steps

The need to act decisively on privacy and consent issues is now - CIPS extends our full support to your Office. We agree with the statement by Privacy Commissioner Therrien '…future uses of data cannot be predicted.[20]' We urge your Office to take swift, direct action to increase efforts around personal privacy and consent. Uncontrolled data collection, use and reuse, in the control of those who may have *no* concerns about individual privacy and reputation, is a looming concern to Canadians. It requires the authority of your Office to find the right answers.

By 2020, the internet of things (IoT) will have 34 billion devices connected to it, through a $6 billion investment[21]. This forecasted growth demonstrates economic opportunities are immense; organizations may not place an emphasis on personal privacy and consent when competing for these dollars. If we are to achieve appropriate levels of personal privacy and reasonable consent, regulatory oversight is necessary to ensure associated economic costs are met.

With all of the above in mind, CIPS hopes to continue the conversation with your Office. We offer our expertise to support your work in protecting the privacy of Canadians.

19 Ibid.

20 From 2016 IAPP Canada Privacy Symposium speech delivered by Privacy Commission Daniel Therrien

21 BI Intelligence Estimates (2015)

Appendix A – CIPS Background

Since its inception in 1958, CIPS has been Canada's association of IT professionals, representing practitioners on issues affecting the profession and our industry. With membership across Canada, CIPS is involved in a number of initiatives related to public policy, setting standards within the IT profession, and assisting our community.

Our main programs are:

- certification of IT practitioners;
- accreditation of computer science, software engineering, and management information systems programs in universities and colleges;
- professional development of our membership through presentations, educational events, and conferences.

In 1989, CIPS established the 'Information Systems Professional of Canada' designation. CIPS members who have met standards of education and experience necessary to be registered as a certified member, are awarded the designation of I.S.P. The I.S.P. is the only IT designation **recognized by law in Canada**.

Following the model of the Professional Engineers Association of Canada, similar requirements for the I.S.P. were stipulated from the beginning for education, professional-level experience and continuing education. A crucial difference however, was our awareness provincial and territorial governments, in 1989, were very unlikely to accept the creation of a new ***licensed*** profession. We have adapted as many of the founding principles of the traditional professions as possible in our I.S.P. designation.

All CIPS members must: abide by the CIPS Code of Ethics; practise only within their areas of competency; remain current with advances in the field.

Certified members (I.S.P. holders) must maintain a peer reviewed professional development program and are answerable to their peers through a formal disciplinary process.

Adherence to the CIPS Code of Ethics and Professional Conduct (CIPS Code of Ethics) is required of all CIPS members.

CIPS members involved in the development, operation, and management of information systems must ensure the application of these systems protects the public interest while also serving the client and/or employer. The CIPS Code of Ethics makes it clear:

> " The obligation to protect the public interest is paramount and must prevail when there is conflict with other obligations."

The complete CIPS Code of Ethics can be viewed here. However we would like to specifically highlight the duty to " understand and comply with any obligations imposed on them under applicable privacy legislation, including The Personal Information Protection and Electronic Documents Act, any amendments to or successor legislation," is included in the Code of Ethics.

Appendix B – CIPS International Contributions

Along with CIPS' established presence across Canada, is our work at the international level.

The International Professional Practice Partnership (IP3) is a global initiative adopted in 2006 by the International Federation of Information Processing (IFIP), a UN founded/UNESCO association; 60+ member Societies attend the annual IFIP General Assembly (GA). IP3 consists of the leading professional IT associations across the globe sharing a common goal: to establish IT as a profession, recognized and valued globally, with the same key strategic features common to most established professions. [CIPS is Canada's representative to IFIP and is a founding member of IP3.]

In 2008, CIPS became the second association in the world to achieve IP3P accreditation status for our ITCP designation. Holders of the ITCP designation are now recognized globally under the IP3P standard. An international perspective is critical in addressing Canada's response to protection of our citizens and our personal information. CIPS' members contributed in a number of ways to the IFIP Global Industry Council Skills Report 2020; we continue to play a key role.

An example of our influence in the ICT profession globally is our contribution to the recently published Global Industry Council (GIC) 2020 ICT Skills Assessment, through our participation in the Global Industry Council (GIC). [The GIC is the principal forum within which industry, IT employers and educators can engage with IP3 to guide development of the IT profession globally.] The GIC was founded by a current CIPS Fellow, several CIPS members sit as directors. This experience, as well as our in-depth stakeholder relationships, places CIPS in a position to partner or even lead development of professional certifications and/or education to support privacy and consent approaches within Canada.

Contacting CIPS

Primary contact person regarding our response is:

Mary Jean Kucerak, CAE
Chief Operating Officer
CIPS National
5090 Explorer Drive, Suite 801
Mississauga, Ontario L4W 4T9

Telephone: (905) 602-1370
Toll Free: 1-877-ASK-CIPS (275-2477)
Fax: (905) 602-7884
E-mail: mj@cips.ca

This response has been supported by the CIPS National Board of Directors with input from CIPS members across Canada. Major contributors were:

Mark Olson, I.S.P., ITCP	CIPS Alberta
David P.J. O'Leary, I.S.P., ITCP	CIPS British Columbia
Lee Anne Davies, PhD., CIPP/c	CIPS British Columbia
Doran Ingalls, LL.B.	CIPS Alberta

Thank-you to the highly qualified reviewers:

Thomas P. Keenan, Ed.D., FCIPS, I.S.P., ITCP	CIPS Alberta
Marilyn Harris, Hon. FCIPS	CIPS British Columbia
Kerry Augustine, I.S.P., ITCP	CIPS Manitoba
Joanne Wong, P.Eng	Montreal